VOLUME 35, NUMBER 4, DECEMBER 2018

ALGEBRAS, GROUPS AND GEOMETRIES Volume 35, Number 4, December 2018

ALGEBRAS, GROUPS AND GEOMETRIES

FOUNDED IN 1984. SOME OF THE PAST EDITORS INCLUDE PROFESSORS: A. A. ANDERSEN, V. V. DEODHAR, J. R. FAULKNER, M. GOLDBERG, N. IWAHORI, M. KOECHER, M. MARCUS, K. M. MCCRIMMON, R. V. MOODY, R. H. OHEMKE, J. M. OSBORN, J. PATERA, H. RUND, T. A. SPRINGER, G. S. TSAGAS.

EDITORIAL BOARD

M.R. ADHIKARI
A.K. ARINGAZIN
P. K. BANERJI
A. BAYOUMI
QING-MING CHENG
A. HARMANCY
L. P. HORWITZ
C. P. JOHNSON
S.L. KALLA
N. KAMIYA
J. LOHMUS*
R. MIRON
M.R. MOLAEI
P. NOWOSAD
KAR-PING SHUM
SERGEI SILVESTROV
H. M. SRIVASTAVA
G.T. TSAGAS*
* In memoriam

FOUNDER and Editor In Chief
R. M. SANTILLI

HADRONIC PRESS, INC.

ALGEBRAS GROUPS AND GEOMETRIES

VOLUME 35, NUMBER 4, DECEMBER 2018

ADDITIVITY OF JORDON n-TUPLE HIGHER DERIVABLE MAPS ON RINGS, 329
João Carlos da Motta Ferreira and Maria das Graças Bruno Marietto
Center for Mathematics, Computation and Cognition,
Federal University of ABC
Santa Adélia Street, 166, 09210-170, Santo André, Brazil
RINGS IN WHICH ELEMENTS ARE A SUM OF A CENTRAL AND NILPOTENT ELEMENT, 347
Yosum Kurtlmaz
Department of Mathematics, Bilkent University, Ankara, Turkey
Abdullah Harmanci
Department of Mathematics, Hacettepe University, Ankara, Turkey
HAMILTON-JACOBI TREATMENT OF SUPERSTRING AND QUANTIZATION OF FIELDS WITH CONSTRAINTS, 365
W. I. Eshraim
Institute for Theoretical Physics, Goethe University, Frankfurt am Main,
Institute for Theoretical Physics, Justus-Liebig University,
Giessen, Germany
ON RIEMANN CONJECTURE, 389
Jiang Yu
Guangzeng Group, fourth floor, number 10,
Guangming East Road, Zengcheng City,
Post Code: 511316, Guangdong Province, China
ISONUMBERS AND RGB IMAGE ENCRYPTION, 395
Mamadou I. Wade and Tepper L. Gill
EECS Howard University, Washington, DC 20059

ON EXTENDED CAMPOPIANO'S TYPE BOUND FOR LPA CODES, 413

Sapna Jain
Shanxi Normal University, P. R. China
K. P. Shum
Institute of Mathematics, Yunnan University, Kunming, 650091
P. R. China

UNIFORMLY INDEPENDENT I-SPOTTY-BYTE ERROR CONTROL CODES, 427

Sapna Jain
Shanxi Normal University, P. R. China

INDEX VOL 45, 2018.....451

ALGEBRAS GROUPS AND GEOMETRIES 35 329 - 346 (2018)
DOI 10.29083/AGG.35.04.2018

ADDITIVITY OF JORDON n-TUPLE HIGHER DERIVABLE MAPS ON RINGS

João Carlos da Motta Ferreira and Maria das Graças Bruno Marietto
Center for Mathematics, Computation and Cognition,
Federal University of ABC
Santa Adélia Street, 166,
09210-170, Santo André, Brazil
joao.cmferreira@ufabc.edu.br
graca.marietto@ufabc.edu.br

Received January 30, 2020

Abstract

Let $\mathscr{R}$ be a ring and $D = \{d_m\}_{m\in\mathbb{N}}$ a family of maps $d_m : \mathscr{R} \to \mathscr{R}$ satisfying $d_0 = I_{\mathscr{R}}$ (the identity map on $\mathscr{R}$) and $d_m(a_n \circ (\cdots (a_2 \circ a_1)\cdots)) = \sum_{p_1+\ldots+p_n=m} d_{p_n}(a_n) \circ (\cdots (d_{p_2}(a_2) \circ d_{p_1}(a_1))\cdots)$, for all $a_1, \cdots, a_n \in \mathscr{R}$ and for each $m \in \mathbb{N}$, where $a \circ b = ab + ba$ is the Jordan product of a and b in $\mathscr{R}$. We prove that if $\mathscr{R}$ contain a non-trivial idempotent satisfying some conditions, then d_m is additive for each $m \in \mathbb{N}$. In particular, if $\mathscr{R}$ is a standard operator algebra, then d_m is additive for each $m \in \mathbb{N}$.

2010 Mathematics Subject Classification. 16W25; 16N60; 47B47.
Keywords. Additivity, Jordan n-tuple higher derivable maps, rings, standard operator algebras.

Copyright © 2018 by Hadronic Press Inc., Palm Harbor, FL 34682, U.S.A.

1 Introduction

A ring $\mathscr{R}$ is called *k-torsion free* if $k\,x = 0$ implies $x = 0$, for any $x \in \mathscr{R}$, where k is a positive integer. We define the *Jordan product* $a \circ b$ of elements a, b in $\mathscr{R}$ as $a \circ b = ab + ba$.

Let $\mathscr{R}$ be a ring and $\delta : \mathscr{R} \to \mathscr{R}$ be a map. We call δ a *derivable map* or *multiplicative derivation* if $\delta(ab) = \delta(a)b + a\delta(b)$ for all $a, b \in \mathscr{R}$, a *Jordan derivable map* or *multiplicative Jordan derivation* if $\delta(a \circ b) = \delta(a) \circ b + a \circ \delta(b)$ for all $a, b \in \mathscr{R}$ and a *Jordan n-tuple derivable map* or *multiplicative Jordan n-tuple derivation* if

$$\delta(a_n \circ (\cdots (a_2 \circ a_1) \cdots)) = \sum_{k=1}^{n} a_n \circ (\cdots (\delta(a_k) \circ (\cdots (a_2 \circ a_1) \cdots)) \cdots)$$

for all $a_1, \cdots, a_n \in \mathscr{R}$.

Let $\mathscr{R}$ be a ring and $D = \{d_m\}_{m \in \mathbb{N}}$ a family of maps $d_m : \mathscr{R} \to \mathscr{R}$, for all $m \in \mathbb{N} = \{0, 1, 2, \cdots\}$, such that $d_0 = I_{\mathscr{R}}$ (the identity map on $\mathscr{R}$). We call D a *Jordan n-tuple higher derivable map* if

$$d_m(a_n \circ (\cdots (a_2 \circ a_1) \cdots)) = \sum_{p_1 + \ldots + p_n = m} d_{p_n}(a_n) \circ (\cdots (d_{p_2}(a_2) \circ d_{p_1}(a_1)) \cdots), \quad (1)$$

for all $a_1, \cdots, a_n \in \mathscr{R}$ and for each $m \in \mathbb{N}$.

We say that a Jordan n-tuple higher derivable map $D = \{d_m\}_{m \in \mathbb{N}}$ is *additive* if d_m is additive, for each $m \in \mathbb{N}$.

The authors in [3] studied the additivity of Jordan 2-tuple derivable maps, defined on rings having at least one non-trivial idempotent, and the authors in [2] extended their results to the Jordan n-tuple derivable maps, for all integers $n \geq 3$ and similar classes of rings. Recently, the authors in [1] studied the additivity of Jordan 2-tuple higher derivable maps for the same class of rings in [3]. They proved the following main theorem:

Theorem 1.1. *[1] Let $\mathscr{R}$ be a ring containing a nontrivial idempotent and satisfying the following conditions for $i, j, k \in \{1, 2\}$.*

(P1) If $a_{ij}x_{jk} = 0$ for all $x_{jk} \in \mathscr{R}_{jk}$, then $a_{ij} = 0$;

(P2) If $x_{ij}a_{jk} = 0$ *for all* $x_{ij} \in \mathscr{R}_{ij}$, *then* $a_{jk} = 0$;

(P3) If $a_{ii}x_{ii} + x_{ii}a_{ii} = 0$ *for all* $x_{ii} \in \mathscr{R}_{ii}$, *then* $a_{ii} = 0$.

If the family $D = \{d_m\}_{m\in\mathbb{N}}$ *of mappings* $d_m : \mathscr{R} \to \mathscr{R}$ *such that* $d_0 = I_{\mathscr{R}}$ *satisfies*

$$d_m(ab + ba) = \sum_{p+q=m} d_p(a)d_q(b) + d_p(b)d_q(a)$$

for all $a, b \in \mathscr{R}$ *and for each* $m \in \mathbb{N}$, *then* $D = \{d_m\}_{m\in\mathbb{N}}$ *is additive. In addition, if* $\mathscr{R}$ *is 2-torsion free, then* $D = \{d_m\}_{m\in\mathbb{N}}$ *is a Jordan higher derivation.*

The aim of this paper is to extend the Theorem 1.1 to the class of Jordan n-tuple higher derivable maps, for all integer $n \geq 3$ and similar classes of rings in [2].

2 The main result

Our main result reads as follows.

Theorem 2.1. *Let* $\mathscr{R}$ *be a ring* 2 *and* $(2^{n-1} - 1)$*-torsion free containing a non-trivial idempotent* e_1 *and satisfying the following conditions:*

(i) $e_iae_j\mathscr{R}e_k = 0$ *or* $e_k\mathscr{R}e_iae_j = 0$ *implies* $e_iae_j = 0$ $(1 \leq i, j, k \leq 2)$;

(ii) $r_{22} \circ (\cdots (a_{22} \circ r_{22}) \cdots) = 0$ *for all* $r_{22} \in \mathscr{R}_{22}$, *implies* $a_{22} = 0$.

Then every Jordan n-tuple higher derivable map $D = \{d_m\}_{m\in\mathbb{N}}$ *is additive.*

Following the ideas and techniques used by Ashraf et al. [1] and Ferreira et al. [2] we shall organize the proof of Theorem 2.1 in a series of lemmas.

We note that for $m = 1$, the identity (1) reduces to

$$d_1(a_n \circ (\cdots (a_2 \circ a_1) \cdots)) = \sum_{i=1}^{n} a_n \circ (\cdots (d_1(a_i) \circ (\cdots (a_2 \circ a_1) \cdots)) \cdots)$$

for all $a_1, \cdots, a_n \in \mathscr{R}$. Thus, from the [2, Theorem 2.1.] d_1 is an additive map. We use this result throughout the paper without further reference.

We begin with the following lemma:

Lemma 2.1. *$d_m(0) = 0$ for each $m \in \mathbb{N}$.*

Proof. We prove the lemma based on second principle of mathematical induction for m. Let's assume that $d_k(0) = 0$ for every non-negative integer k with $k < m$ for any non-negative integer m. It follows that

$$\begin{aligned} d_m(0) &= d_m(\underbrace{0 \circ (\cdots (0 \circ 0) \cdots)}_{n-\text{times}}) \\ &= \sum_{p_1+\ldots+p_n=m} d_{p_n}(0) \circ (\cdots (d_{p_2}(0) \circ d_{p_1}(0)) \cdots) \\ &= 0 \circ (\cdots (d_m(0) \circ 0) \cdots) \\ &\quad + \sum_{\substack{p_1+\ldots+p_n=m \\ p_2 \neq m}} d_{p_n}(0) \circ (\cdots (d_{p_2}(0) \circ d_{p_1}(0)) \cdots) = 0. \end{aligned}$$

Therefore, we can conclude that $d_m(0) = 0$, for each nonnegative integer m. □

In what follows, we assume the assumption that d_k is an additive map for each non-negative integer $k < m$ for any non-negative integer m.

The following lemma will be used throughout this paper, whose proof is elementary and therefore omitted.

Lemma 2.2. *For any elements $a_{11} \in \mathscr{R}_{11}$, $b_{12} \in \mathscr{R}_{12}$, $c_{21} \in \mathscr{R}_{21}$ and $d_{22} \in \mathscr{R}_{22}$ the following holds*

$$\begin{aligned} & d_m(r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots ((a_{11} + b_{12} + c_{21} + d_{22}) \circ r^1_{i_1j_1}) \cdots)) \\ = & \sum_{p_1+\ldots+p_n=m} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}}) \circ (\cdots (d_{p_k}(r^k_{i_kj_k}) \\ & \qquad \circ (\cdots (d_{p_2}(a_{11} + b_{12} + c_{21} + d_{22}) \circ d_{p_1}(r^1_{i_1j_1})) \cdots)) \cdots) \\ = & \; r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots (d_m(a_{11} + b_{12} + c_{21} + d_{22}) \circ r^1_{i_1j_1}) \cdots) \\ & + \sum_{\substack{p_1+\ldots+p_n=m \\ p_2 \neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}}) \circ (\cdots (d_{p_k}(r^k_{i_kj_k}) \\ & \qquad \circ (\cdots (d_{p_2}(a_{11}) \circ d_{p_1}(r^1_{i_1j_1})) \cdots)) \cdots) \end{aligned}$$

$$
\begin{aligned}
&+ \sum_{\substack{p_1+\ldots+p_n=m \\ p_2\neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}}) \circ (\cdots (d_{p_k}(r^k_{i_kj_k}) \\
&\qquad \circ(\cdots (d_{p_2}(b_{12}) \circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots) \\
&+ \sum_{\substack{p_1+\ldots+p_n=m \\ p_2\neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}}) \circ (\cdots (d_{p_k}(r^k_{i_kj_k}) \\
&\qquad \circ(\cdots (d_{p_2}(c_{21}) \circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots) \\
&+ \sum_{\substack{p_1+\ldots+p_n=m \\ p_2\neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}}) \circ (\cdots (d_{p_k}(r^k_{i_kj_k}) \\
&\qquad \circ(\cdots (d_{p_2}(d_{22}) \circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots) \qquad (2)
\end{aligned}
$$

for all $r^k_{i_kj_k} \in \mathscr{R}_{i_kj_k}$ $(i_k, j_k = 1, 2; k = 1, \cdots n-1)$.

Lemma 2.3. *For any elements* $a_{11} \in \mathscr{R}_{11}$, $b_{12} \in \mathscr{R}_{12}$, $c_{21} \in \mathscr{R}_{21}$ *and* $d_{22} \in \mathscr{R}_{22}$ *the following hold: (i)* $d_m(a_{11} + b_{12}) = d_m(a_{11}) + d_m(b_{12})$; *(ii)* $d_m(a_{11} + c_{21}) = d_m(a_{11}) + d_m(c_{21})$; *(iii)* $d_m(b_{12} + d_{22}) = d_m(b_{12}) + d_m(d_{22})$ *and (iv)* $d_m(c_{21} + d_{22}) = d_m(c_{21}) + d_m(d_{22})$.

Proof. For any elements $r^k_{i_kj_k} \in \mathscr{R}_{i_kj_k}$ $(k = 1, \cdots, n-1)$, with $(i_1, j_1) = (1, 1)$ and $(i_k, j_k) = (2, 2)$ $(k = 2, \cdots, n-1)$, or $(i_k, j_k) = (2, 2)$ $(k = 1, \cdots, n-1)$, or $(i_1, j_1) = (1, 2)$ and $(i_k, j_k) = (2, 2)$ $(k = 2, \cdots, n-1)$, we have

$$
\begin{aligned}
& d_m(r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots ((a_{11} + b_{12}) \circ r^1_{i_1j_1})\cdots)) \\
= \; & d_m(r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots (a_{11} \circ r^1_{i_1j_1})\cdots)) \\
& + d_m(r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots (b_{12} \circ r^1_{i_1j_1})\cdots)) \\
= \; & \sum_{p_1+\ldots+p_n=m} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}}) \circ (\cdots (d_{p_k}(r^k_{i_kj_k}) \\
& \qquad \circ(\cdots (d_{p_2}(a_{11}) \circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots) \\
& + \sum_{p_1+\ldots+p_n=m} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}}) \circ (\cdots (d_{p_k}(r^k_{i_kj_k}) \\
& \qquad \circ(\cdots (d_{p_2}(b_{12}) \circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots) \\
= \; & r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots (d_m(a_{11}) \circ r^1_{i_1j_1})\cdots)
\end{aligned}
$$

$$
\begin{aligned}
&+ \sum_{\substack{p_1+\ldots+p_n=m \\ p_2\neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}}) \circ (\cdots (d_{p_k}(r^k_{i_kj_k}) \\
&\qquad \circ(\cdots (d_{p_2}(a_{11}) \circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots) \\
&+r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots (d_m(b_{12}) \circ r^1_{i_1j_1})\cdots) \\
&+ \sum_{\substack{p_1+\ldots+p_n=m \\ p_2\neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}}) \circ (\cdots (d_{p_k}(r^k_{i_kj_k}) \\
&\qquad \circ(\cdots (d_{p_2}(b_{12}) \circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots). \qquad (3)
\end{aligned}
$$

Considering $c_{21} = d_{22} = 0$ in (2) and subtracting (2) from (3), we obtain

$$r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots ((d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12})) \circ r^1_{i_1j_1})\cdots) = 0. \qquad (4)$$

This implies that, if $(i_1, j_1) = (1, 1)$ and $(i_k, j_k) = (2, 2)$ $(k = 2, \cdots, n-1)$, then we obtain

$$
\begin{aligned}
&r^1_{11}(d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12}))r^2_{22}\cdots r^{n-1}_{22} \\
&\qquad + r^{n-1}_{22}\cdots r^2_{22}(d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12}))r^1_{11} = 0,
\end{aligned}
$$

by (4), which yields

$$
\begin{aligned}
&r^1_{11}(d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12}))r^2_{22}\cdots r^{n-1}_{22} \\
&\qquad = r^{n-1}_{22}\cdots r^2_{22}(d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12}))r^1_{11} = 0.
\end{aligned}
$$

It follows that $(d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12}))_{12} = (d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12}))_{21} = 0$, by [2, Lemma 2.1.(i)]. If $(i_k, j_k) = (2, 2)$ for all $(k = 1, \cdots, n-1)$, then by (4), we obtain

$$r^{n-1}_{22} \circ (\cdots ((d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12})) \circ r^1_{22})\cdots) = 0$$

which yields $(d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12}))_{22} = 0$, by [2, Lemma 2.1.(ii)]. If $(i_1, j_1) = (1, 2)$ and $(i_k, j_k) = (2, 2)$ $(k = 2, \cdots, n-2)$, then by (4) again and the previous cases, we obtain

$$(d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12}))r^1_{12}r^2_{22}\cdots r^{n-1}_{22} = 0$$

which shows that $(d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12}))_{11} = 0$, by [2, Lemma 2.1.(i)]. Consequently, $d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12}) = 0$.

Similarly, we prove (ii), (iii) and (iv). □

Lemma 2.4. *For any elements $a_{12}, b_{12} \in \mathscr{R}_{12}$, $b_{21}, c_{21} \in \mathscr{R}_{21}$ and $t_{22} \in \mathscr{R}_{22}$ the following hold: (i) $d_m(a_{12}t_{22} + b_{12}t_{22}) = d_m(a_{12}t_{22}) + d_m(b_{12}t_{22})$; (ii) $d_m(t_{22}b_{21} + t_{22}c_{21}) = d_m(t_{22}b_{21}) + d_m(t_{22}c_{21})$.*

Proof. First, we observe that the following identity holds

$$a_{12}t_{22} + b_{12}t_{22} = \underbrace{e_1 \circ (\cdots (e_1}_{(n-2)-\text{times}} \circ ((a_{12} + t_{22}) \circ (b_{12} + t_{22}))) \cdots).$$

As a result, we have by Lemma 2.3(iii) that

$$\begin{aligned}
& d_m(a_{12}t_{22} + b_{12}t_{22}) \\
= \; & d_m(\underbrace{e_1 \circ (\cdots (e_1}_{(n-2)-\text{times}} \circ ((a_{12} + t_{22}) \circ (b_{12} + t_{22}))) \cdots)) \\
= \; & \underbrace{e_1 \circ (\cdots (e_1}_{(n-2)-\text{times}} \circ ((a_{12} + t_{22}) \circ d_m(b_{12} + t_{22}))) \cdots) \\
& + \underbrace{e_1 \circ (\cdots (e_1}_{(n-2)-\text{times}} \circ (d_m(a_{12} + t_{22}) \circ (b_{12} + t_{22}))) \cdots) \\
& + \sum_{\substack{p_1+\ldots+p_n=m \\ p_1 \neq m,\ p_2 \neq m}} \underbrace{d_{p_n}(e_1) \circ (\cdots (d_{p_3}(e_1)}_{(n-2)-\text{times}} \\
& \qquad \circ (d_{p_2}(a_{12} + t_{22}) \circ d_{p_1}(b_{12} + t_{22}))) \cdots) \\
= \; & e_1 \circ (\cdots (e_1 \circ (a_{12} \circ d_m(b_{12}))) \cdots) \\
& + e_1 \circ (\cdots (e_1 \circ (a_{12} \circ d_m(t_{22}))) \cdots) \\
& + e_1 \circ (\cdots (e_1 \circ (t_{22} \circ d_m(b_{12}))) \cdots) \\
& + e_1 \circ (\cdots (e_1 \circ (t_{22} \circ d_m(t_{22}))) \cdots) \\
& + e_1 \circ (\cdots (e_1 \circ (d_m(a_{12}) \circ b_{12})) \cdots) \\
& + e_1 \circ (\cdots (e_1 \circ (d_m(a_{12}) \circ t_{22})) \cdots) \\
& + e_1 \circ (\cdots (e_1 \circ (d_m(t_{22}) \circ b_{12})) \cdots) \\
& + e_1 \circ (\cdots (e_1 \circ (d_m(t_{22}) \circ t_{22})) \cdots) \\
& + \sum_{\substack{p_1+\ldots+p_n=m \\ p_1 \neq m,\ p_2 \neq m}} d_{p_n}(e_1) \circ (\cdots (d_{p_k}(e_1) \circ (\cdots (d_{p_2}(a_{12}) \circ d_{p_1}(b_{12})) \cdots)) \cdots)
\end{aligned}$$

$$
\begin{aligned}
&+ \sum_{\substack{p_1+\cdots+p_n=m \\ p_1\neq m,\ p_2\neq m}} d_{p_n}(e_1)\circ(\cdots(d_{p_k}(e_1)\circ(\cdots(d_{p_2}(a_{12})\circ d_{p_1}(t_{22}))\cdots))\cdots) \\
&+ \sum_{\substack{p_1+\cdots+p_n=m \\ p_1\neq m,\ p_2\neq m}} d_{p_n}(e_1)\circ(\cdots(d_{p_k}(e_1)\circ(\cdots(d_{p_2}(t_{22})\circ d_{p_1}(b_{12}))\cdots))\cdots) \\
&+ \sum_{\substack{p_1+\cdots+p_n=m \\ p_1\neq m,\ p_2\neq m}} d_{p_n}(e_1)\circ(\cdots(d_{p_k}(e_1)\circ(\cdots(d_{p_2}(t_{22})\circ d_{p_1}(t_{22}))\cdots))\cdots) \\
= \ & d_m(e_1\circ(\cdots(e_1\circ(a_{12}\circ b_{12}))\cdots)) + d_m(e_1\circ(\cdots(e_1\circ(a_{12}\circ t_{22}))\cdots)) \\
& + d_m(e_1\circ(\cdots(e_1\circ(t_{22}\circ b_{12}))\cdots)) + d_m(e_1\circ(\cdots(e_1\circ(t_{22}\circ t_{22}))\cdots)) \\
= \ & d_m(a_{12}t_{22}) + d_m(b_{12}t_{22}).
\end{aligned}
$$

Using a similar argument to the previous case we prove that $d_m(t_{22}b_{21} + t_{22}c_{21}) = d_m(t_{22}b_{21}) + d_m(t_{22}c_{21})$, from the identity

$$
t_{22}b_{21} + t_{22}c_{21} = \underbrace{e_1\circ(\cdots(e_1}_{(n-2)-\text{times}}\circ((c_{21}+t_{22})\circ(b_{21}+t_{22})))\cdots).
$$

□

Lemma 2.5. *For any elements $a_{12}, b_{12} \in \mathscr{R}_{12}$ and $b_{21}, c_{21} \in \mathscr{R}_{21}$ the following hold: (i) $d_m(a_{12}+b_{12}) = d_m(a_{12}) + d_m(b_{12})$; (ii) $d_m(b_{21}+c_{21}) = d_m(b_{21}) + d_m(c_{21})$.*

Proof. For any elements $r^k_{i_kj_k} \in \mathscr{R}_{i_kj_k}$ $(k = 1, \cdots, n-1)$ with $(i_1, j_1) = (1,1)$ and $(i_k, j_k) = (2,2)$ $(k = 2, \cdots, n-1)$, or $(i_k, j_k) = (2,2)$ $(k = 1, \cdots, n-1)$, or $(i_1, j_1) = (1,2)$ and $(i_k, j_k) = (2,2)$ $(k = 2, \cdots, n-1)$, we have by Lemma 2.4(i) that

$$
\begin{aligned}
& d_m(r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots((a_{12}+b_{12})\circ r^1_{i_1j_1})\cdots)) \\
= \ & d_m(r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots(a_{12}\circ r^1_{i_1j_1})\cdots)) \\
& + d_m(r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots(b_{12}\circ r^1_{i_1j_1})\cdots)) \\
= \ & r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots(d_m(a_{12})\circ r^1_{i_1j_1})\cdots) \\
& + \sum_{\substack{p_1+\cdots+p_n=m \\ p_2\neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}})\circ(\cdots(d_{p_k}(r^k_{i_kj_k})
\end{aligned}
$$

$$\begin{aligned}
&\circ(\cdots(d_{p_2}(a_{12})\circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots)\\
&+r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots(d_m(b_{12})\circ r^1_{i_1j_1})\cdots)\\
&+\sum_{\substack{p_1+\ldots+p_n=m\\ p_2\neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}})\circ(\cdots(d_{p_k}(r^k_{i_kj_k})\\
&\qquad\circ(\cdots(d_{p_2}(b_{12})\circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots). \qquad (5)
\end{aligned}$$

Considering $a_{11}=c_{21}=d_{22}=0$ and replacing b_{12} by $a_{12}+b_{12}$, in (2), and subtracting (2) from (5), it results

$$r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots((d_m(a_{12}+b_{12})-d_m(a_{12})-d_m(b_{12}))\circ r^1_{i_1j_1})\cdots)=0. \quad (6)$$

As a consequence, if $(i_1,j_1)=(1,1)$ and $(i_k,j_k)=(2,2)$ $(k=2,\cdots,n-1)$ we get

$$\begin{aligned}
&r^1_{11}(d_m(a_{12}+b_{12})-d_m(a_{12})-d_m(b_{12}))r^2_{22}\cdots r^{n-1}_{22}\\
&\qquad+r^{n-1}_{22}\cdots r^2_{22}(d_m(a_{12}+b_{12})-d_m(a_{12})-d_m(b_{12}))r^1_{11}=0,
\end{aligned}$$

by (6), which results that

$$\begin{aligned}
&r^1_{11}(d_m(a_{12}+b_{12})-d_m(a_{12})-d_m(b_{12}))r^2_{22}\cdots r^{n-1}_{22}\\
&\qquad=r^{n-1}_{22}\cdots r^2_{22}(d_m(a_{12}+b_{12})-d_m(a_{12})-d_m(b_{12}))r^1_{11}=0.
\end{aligned}$$

It implies that $(d_m(a_{12}+b_{12})-d_m(a_{12})-d_m(b_{12}))_{12}=(d_m(a_{12}+b_{12})-d_m(a_{12})-d_m(b_{12}))_{21}=0$. If $(i_k,j_k)=(2,2)$ for all $(k=1,\cdots,n-1)$, then by (6), we obtain

$$r^{n-1}_{22}\circ(\cdots((d_m(a_{12}+b_{12})-d_m(a_{12})-d_m(b_{12}))\circ r^1_{22})\cdots)=0.$$

which results $(d_m(a_{12}+b_{12})-d_m(a_{12})-d_m(b_{12}))_{22}=0$, by [2, Lema 2.1.(ii)]. If $(i_1,j_1)=(1,2)$ and $(i_k,j_k)=(2,2)$ $(k=2,\cdots,n-1)$, then by (6) and the previous cases, we conclude that

$$(d_m(a_{12}+b_{12})-d_m(a_{12})-d_m(b_{12}))r^1_{12}r^2_{22}\cdots r^{n-1}_{22}=0.$$

It therefore follows that $(d_m(a_{12}+b_{12})-d_m(a_{12})-d_m(b_{12}))_{11}=0$. Consequently, $d_m(a_{12}+b_{12})-d_m(a_{12})-d_m(b_{12})=0$.

Similarly, we prove (ii). □

Lemma 2.6. *For any elements $a_{11}, b_{11} \in \mathscr{R}_{11}$ and $c_{22}, d_{22} \in \mathscr{R}_{22}$ the following hold: (i) $d_m(a_{11}+b_{11}) = d_m(a_{11}) + d_m(b_{11})$; (ii) $d_m(c_{22}+d_{22}) = d_m(c_{22}) + d_m(d_{22})$.*

Proof. For any elements $r^k_{i_kj_k} \in \mathscr{R}_{i_kj_k}$ $(k = 1, \cdots, n-1)$ with $(i_1, j_1) = (1,1)$ and $(i_k, j_k) = (2,2)$ $(k = 2, \cdots, n-1)$, or $(i_k, j_k) = (2,2)$ $(k = 1, \cdots, n-1)$, or $(i_1, j_1) = (1,2)$ and $(i_k, j_k) = (2,2)$ $(k = 2, \cdots, n-1)$, we have by Lemma 2.5(i) that

$$\begin{aligned}
& d_m(r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots((a_{11}+b_{11}) \circ r^1_{i_1j_1})\cdots)) \\
= \; & d_m(r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots(a_{11} \circ r^1_{i_1j_1})\cdots)) \\
& + d_m(r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots(b_{11} \circ r^1_{i_1j_1})\cdots)) \\
= \; & r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots(d_m(a_{11}) \circ r^1_{i_1j_1})\cdots) \\
& + \sum_{\substack{p_1+\ldots+p_n=m \\ p_2 \neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}}) \circ (\cdots(d_{p_k}(r^k_{i_kj_k}) \\
& \qquad \circ(\cdots(d_{p_2}(a_{11}) \circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots) \\
& + r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots(d_m(b_{11}) \circ r^1_{i_1j_1})\cdots) \\
& + \sum_{\substack{p_1+\ldots+p_n=m \\ p_2 \neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}}) \circ (\cdots(d_{p_k}(r^k_{i_kj_k}) \\
& \qquad \circ(\cdots(d_{p_2}(b_{11}) \circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots). \qquad (7)
\end{aligned}$$

Considering $b_{12} = c_{21} = d_{22} = 0$ and replacing a_{11} by $a_{11} + b_{11}$, in (2), and subtracting (2) from (7), we get

$$r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots((d_m(a_{11}+b_{11}) - d_m(a_{11}) - d_m(b_{11})) \circ r^1_{i_1j_1})\cdots) = 0. \quad (8)$$

As a consequence, if $(i_1, j_1) = (1,1)$ and $(i_k, j_k) = (2,2)$ $(k = 2, \cdots, n-1)$, by (8) we obtain

$$\begin{aligned}
& r^1_{11}(d_m(a_{11}+b_{11}) - d_m(a_{11}) - d_m(b_{11}))r^2_{22}\cdots r^{n-1}_{22} \\
& \qquad = r^{n-1}_{22}\cdots r^2_{22}(d_m(a_{11}+b_{11}) - d_m(a_{11}) - d_m(b_{11}))r^1_{11} = 0.
\end{aligned}$$

which shows that $(d_m(a_{11}+b_{11}) - d_m(a_{11}) - d_m(b_{11}))_{12} = (d_m(a_{11}+b_{11}) - d_m(a_{11}) - d_m(b_{11}))_{21} = 0$. If $(i_k, j_k) = (2,2)$ for all $(k = 1, \cdots, n-1)$, then

by (8), we obtain

$$r_{22}^{n-1} \circ (\cdots((d_m(a_{11}+b_{11}) - d_m(a_{11}) - d_m(b_{11})) \circ r_{22}^1)\cdots) = 0$$

resulting in $(d_m(a_{11}+b_{11}) - d_m(a_{11}) - d_m(b_{11}))_{22} = 0$, by [2, Lema 2.1.(ii)]. If $(i_1, j_1) = (1,2)$ and $(i_k, j_k) = (2,2)$ $(k = 2, \cdots, n-1)$, then by (8) yet and the previous cases, we obtain

$$(d_m(a_{11}+b_{11}) - d_m(a_{11}) - d_m(b_{11}))r_{12}^1 r_{22}^2 \cdots r_{22}^{n-1} = 0$$

which results that $(d_m(a_{11}+b_{11}) - d_m(a_{11}) - d_m(b_{11}))_{11} = 0$. Consequently, $d_m(a_{11}+b_{11}) - d_m(a_{11}) - d_m(b_{11}) = 0$.

Similarly, we prove (ii). □

Lemma 2.7. *For any elements $b_{12} \in \mathscr{R}_{12}$ and $c_{21} \in \mathscr{R}_{21}$ the following holds $d_m(b_{12}+c_{21}) = d_m(b_{12}) + d_m(c_{21})$.*

Proof. For any elements $r_{i_k j_k}^k \in \mathscr{R}_{i_k j_k}$ $(k = 1, \cdots, n-1)$ with $(i_{n-1}, j_{n-1}) = (1,2)$ and $(i_k, j_k) = (1,1)$ $(k = 1, \cdots, n-2)$, or $(i_{n-1}, j_{n-1}) = (2,1)$ and $(i_k, j_k) = (2,2)$ $(k = 1, \cdots, n-2)$, or $(i_1, j_1) = (1,2)$ and $(i_k, j_k) = (1,1)$ $(k = 2, \cdots, n-1)$, we have

$$\begin{aligned}
& d_m(r_{i_{n-1}j_{n-1}}^{n-1} \circ (\cdots((b_{12}+c_{21}) \circ r_{i_1 j_1}^1)\cdots)) \\
= \; & d_m(r_{i_{n-1}j_{n-1}}^{n-1} \circ (\cdots(b_{12} \circ r_{i_1 j_1}^1)\cdots)) \\
& + d_m(r_{i_{n-1}j_{n-1}}^{n-1} \circ (\cdots(c_{21} \circ r_{i_1 j_1}^1)\cdots)) \\
= \; & r_{i_{n-1}j_{n-1}}^{n-1} \circ (\cdots(d_m(b_{12}) \circ r_{i_1 j_1}^1)\cdots) \\
& + \sum_{\substack{p_1+\ldots+p_n=m \\ p_2 \neq m}} d_{p_n}(r_{i_{n-1}j_{n-1}}^{n-1}) \circ (\cdots(d_{p_k}(r_{i_k j_k}^k) \\
& \qquad \circ(\cdots(d_{p_2}(b_{12}) \circ d_{p_1}(r_{i_1 j_1}^1))\cdots))\cdots) \\
& + r_{i_{n-1}j_{n-1}}^{n-1} \circ (\cdots(d_m(c_{21}) \circ r_{i_1 j_1}^1)\cdots) \\
& + \sum_{\substack{p_1+\ldots+p_n=m \\ p_2 \neq m}} d_{p_n}(r_{i_{n-1}j_{n-1}}^{n-1}) \circ (\cdots(d_{p_k}(r_{i_k j_k}^k) \\
& \qquad \circ(\cdots(d_{p_2}(c_{21}) \circ d_{p_1}(r_{i_1 j_1}^1))\cdots))\cdots). \qquad (9)
\end{aligned}$$

Considering $a_{11} = d_{22} = 0$ in (2) and subtracting (2) from (9) we get

$$r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots((d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21})) \circ r^1_{i_1 j_1})\cdots) = 0. \quad (10)$$

As a consequence, if $(i_{n-1}, j_{n-1}) = (1,2)$ and $(i_k, j_k) = (1,1)$ $(k = 1, \cdots, n-2)$ we obtain

$$r^{n-1}_{12} \circ (r^{n-2}_{11} \circ (\cdots((d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21})) \circ r^1_{11})\cdots)) = 0, \quad (11)$$

by (10). Multiplying (11) from right by t_{11}, then

$$r^{n-1}_{12}((d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21}))r^1_{11}\cdots r^{n-2}_{11}t_{11} = 0$$

which results that $d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21}))_{21} = 0$. If $(i_{n-1}, j_{n-1}) = (2,1)$ and $(i_k, j_k) = (2,2)$ $(k = 1, \cdots, n-2)$ we obtain

$$r^{n-1}_{21} \circ (r^{n-2}_{22} \circ (\cdots((d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21})) \circ r^1_{22})\cdots)) = 0, \quad (12)$$

by (10) again. Multiplying (12) from right by t_{22}, then

$$r^{n-1}_{21}((d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21}))r^1_{22}\cdots r^{n-2}_{22}t_{22} = 0$$

which yields that $(d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21}))_{12} = 0$. Now, let us prove that $(d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21}))_{11} = 0$. First, we observe that the following identity holds $b_{12} + c_{21} = \underbrace{e_1 \circ (\cdots((b_{12}+c_{21}) \circ e_1)\cdots)}_{n-\text{times}}$. As consequence, we have

$$\begin{aligned} d_m(b_{12}+c_{21}) = &= d_m(\underbrace{e_1 \circ (\cdots((b_{12}+c_{21}) \circ e_1)\cdots)}_{n-\text{times}}) \\ &= e_1 \circ (\cdots(d_m(b_{12}+c_{21}) \circ e_1)\cdots) \\ &\quad + \sum_{\substack{p_1+\ldots+p_n=m \\ p_2 \neq m}} d_{p_n}(e_1) \circ (\cdots(d_{p_k}(e_1) \\ &\qquad \circ(\cdots(d_{p_2}(b_{12}+c_{21}) \circ d_{p_1}(e_1))\cdots))\cdots) \end{aligned}$$

$$
\begin{aligned}
&= e_1 \circ (\cdots (d_m(b_{12}+c_{21}) \circ e_1) \cdots) \\
&\quad + \sum_{\substack{p_1+\ldots+p_n=m \\ p_2 \neq m}} d_{p_n}(e_1) \circ (\cdots (d_{p_k}(e_1) \\
&\qquad \circ (\cdots (d_{p_2}(b_{12}) \circ d_{p_1}(e_1)) \cdots)) \cdots) \\
&\quad + \sum_{\substack{p_1+\ldots+p_n=m \\ p_2 \neq m}} d_{p_n}(e_1) \circ (\cdots (d_{p_k}(e_1) \\
&\qquad \circ (\cdots (d_{p_2}(c_{21}) \circ d_{p_1}(e_1)) \cdots)) \cdots). \qquad (13)
\end{aligned}
$$

Also, we observe that the identity holds $b_{12} = \underbrace{e_1 \circ (\cdots (b_{12} \circ e_1)}_{n-\text{times}} \cdots)$ which results in,

$$
\begin{aligned}
d_m(b_{12}) &= d_m(\underbrace{e_1 \circ (\cdots (b_{12} \circ e_1)}_{n-\text{times}} \cdots)) \\
&= e_1 \circ (\cdots (d_m(b_{12}) \circ e_1) \cdots) \\
&\quad + \sum_{\substack{p_1+\ldots+p_n=m \\ p_2 \neq m}} d_{p_n}(e_1) \circ (\cdots (d_{p_k}(e_1) \\
&\qquad \circ (\cdots (d_{p_2}(b_{12}) \circ d_{p_1}(e_1)) \cdots)) \cdots). \qquad (14)
\end{aligned}
$$

Similarly, we have $c_{21} = \underbrace{e_1 \circ (\cdots (c_{21} \circ e_1)}_{n-\text{times}} \cdots)$ which yields

$$
\begin{aligned}
d_m(c_{21}) &= d_m(\underbrace{e_1 \circ (\cdots (c_{21} \circ e_1)}_{n-\text{times}} \cdots)) \\
&= e_1 \circ (\cdots (d_m(c_{21}) \circ e_1) \cdots) \\
&\quad + \sum_{\substack{p_1+\ldots+p_n=m \\ p_2 \neq m}} d_{p_n}(e_1) \circ (\cdots (d_{p_k}(e_1) \\
&\qquad \circ (\cdots (d_{p_2}(c_{21}) \circ d_{p_1}(e_1)) \cdots)) \cdots). \qquad (15)
\end{aligned}
$$

It therefore follows that, subtracting (13) from (14) and (15) we obtain

$$d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21})$$

$$= \quad e_1 \circ (\cdots((d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21})) \circ e_1)\cdots). \qquad (16)$$

which implies that $(2^{n-1}-1)e_1(d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21}))e_1 = 0$. As results, we obtain $(d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21}))_{11} = 0$, since $\mathscr{R}$ is a $(2^{n-1}-1)$-torsion free ring. Finally, if $(i_1, j_1) = (1,2)$ and $(i_k, j_k) = (1,1)$ $(k = 2, \cdots, n-1)$, by (10) yet, we have

$$r_{11}^{n-1} \circ (r_{11}^{n-2} \circ (\cdots((d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21})) \circ r_{12}^1)\cdots)) = 0.$$

which shows that

$$r_{11}^{n-1} \cdots r_{11}^2 r_{12}^1 (d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21})) = 0. \qquad (17)$$

The identity (17) allows us to conclude that $(d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21}))_{22} = 0$. Consequently, $d_m(b_{12}+c_{21}) - d_m(b_{12}) - d_m(c_{21}) = 0$. □

Lemma 2.8. *For any elements $a_{11} \in \mathscr{R}_{11}$, $b_{12} \in \mathscr{R}_{12}$, $c_{21} \in \mathscr{R}_{21}$ and $d_{22} \in \mathscr{R}_{22}$ the following hold: (i) $d_m(a_{11}+b_{12}+c_{21}) = d_m(a_{11}) + d_m(b_{12}) + d_m(c_{21})$; (ii) $d_m(b_{12}+c_{21}+d_{22}) = d_m(b_{12}) + d_m(c_{21}) + d_m(d_{22})$.*

Proof. For any elements $r_{i_k j_k}^k \in \mathscr{R}_{i_k j_k}$ $(k = 1, \cdots, n-1)$ with $(i_1, j_1) = (1,1)$ and $(i_k, j_k) = (2,2)$ $(k = 2, \cdots, n-1)$, or $(i_k, j_k) = (2,2)$ $(k = 1, \cdots, n-1)$, or $(i_1, j_1) = (1,2)$ and $(i_k, j_k) = (2,2)$ $(k = 2, \cdots, n-1)$, we have by Lemma 2.7 that

$$\begin{aligned}
& d_m(r_{i_{n-1}j_{n-1}}^{n-1} \circ (\cdots((a_{11}+b_{12}+c_{21}) \circ r_{i_1 j_1}^1)\cdots)) \\
= \; & d_m(r_{i_{n-1}j_{n-1}}^{n-1} \circ (\cdots(a_{11} \circ r_{i_1 j_1}^1)\cdots)) \\
& + d_m(r_{i_{n-1}j_{n-1}}^{n-1} \circ (\cdots(b_{12} \circ r_{i_1 j_1}^1)\cdots)) \\
& + d_m(r_{i_{n-1}j_{n-1}}^{n-1} \circ (\cdots(c_{21} \circ r_{i_1 j_1}^1)\cdots)) \\
= \; & r_{i_{n-1}j_{n-1}}^{n-1} \circ (\cdots(d_m(a_{11}) \circ r_{i_1 j_1}^1)\cdots) \\
& + \sum_{\substack{p_1+\ldots+p_n=m \\ p_2 \neq m}} d_{p_n}(r_{i_{n-1}j_{n-1}}^{n-1}) \circ (\cdots(d_{p_k}(r_{i_k j_k}^k) \\
& \qquad \circ(\cdots(d_{p_2}(a_{11}) \circ d_{p_1}(r_{i_1 j_1}^1))\cdots))\cdots) \\
& + r_{i_{n-1}j_{n-1}}^{n-1} \circ (\cdots(d_m(b_{12}) \circ r_{i_1 j_1}^1)\cdots)
\end{aligned}$$

$$
\begin{aligned}
&+ \sum_{\substack{p_1+\ldots+p_n=m \\ p_2\neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}}) \circ (\cdots (d_{p_k}(r^k_{i_kj_k}) \\
&\qquad \circ(\cdots (d_{p_2}(b_{12}) \circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots) \\
&+r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots (d_m(c_{21}) \circ r^1_{i_1j_1})\cdots) \\
&+ \sum_{\substack{p_1+\ldots+p_n=m \\ p_2\neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}}) \circ (\cdots (d_{p_k}(r^k_{i_kj_k}) \\
&\qquad \circ(\cdots (d_{p_2}(c_{21}) \circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots). \qquad (18)
\end{aligned}
$$

Considering $d_{22} = 0$ in (2) and subtracting (2) from (18), we obtain

$$
\begin{aligned}
&r^{n-1}_{i_{n-1}j_{n-1}} \circ (\cdots ((d_m(a_{11}+b_{12}+c_{21}) \\
&\qquad - d_m(a_{11}) - d_m(b_{11}) - d_m(c_{21})) \circ r^1_{i_1j_1})\cdots) = 0. \qquad (19)
\end{aligned}
$$

As a consequence, if $(i_1, j_1) = (1, 1)$ and $(i_k, j_k) = (2, 2)$ $(k = 2, \cdots, n-1)$, by (19) we get

$$
\begin{aligned}
&r^1_{11}(d_m(a_{11}+b_{12}+c_{21}) - d_m(a_{11}) - d_m(b_{12}) - d_m(c_{21}))r^2_{22}\cdots r^{n-1}_{22} \\
&+ r^{n-1}_{22}\cdots r^2_{22}(d_m(a_{11}+b_{12}+c_{21}) - d_m(a_{11}) - d_m(b_{12}) - d_m(c_{21}))r^1_{11} = 0
\end{aligned}
$$

which implies that

$$
\begin{aligned}
&r^1_{11}(d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12}) - d_m(c_{21}))r^2_{22}\cdots r^{n-1}_{22} \\
&\quad = r^{n-1}_{22}\cdots r^2_{22}(d_m(a_{11}+b_{12}) - d_m(a_{11}) - d_m(b_{12}) - d_m(c_{21}))r^1_{11} = 0.
\end{aligned}
$$

It therefore follows that

$$
\begin{aligned}
&(d_m(a_{11}+b_{12}+c_{21}) - d_m(a_{11}) - d_m(b_{12}) - d_m(c_{21}))_{12} \\
&\qquad = (d_m(a_{11}+b_{12}+c_{21}) - d_m(a_{11}) - d_m(b_{12}) - d_m(c_{21}))_{21} = 0.
\end{aligned}
$$

If $(i_k, j_k) = (2, 2)$ for all $(k = 1, \cdots, n-1)$, then by (19), we get

$$
\begin{aligned}
&r^{n-1}_{22} \circ (\cdots (d_m(a_{11}+b_{12}+c_{21}) \\
&\qquad - d_m(a_{11}) - d_m(b_{12}) - d_m(c_{21})) \circ r^1_{22})\cdots) = 0.
\end{aligned}
$$

which shows that $(d_m(a_{11}+b_{12}+c_{21})-d_m(a_{11})-d_m(b_{12})-d_m(c_{21}))_{22}=0$, by [2, Lema 2.1.(ii)]. If $(i_1,j_1)=(1,2)$ and $(i_k,j_k)=(2,2)$ $(k=2,\cdots,n-1)$, then by (19) we have

$$(d_m(a_{11}+b_{12}+c_{21})-d_m(a_{11})-d_m(b_{12})-d_m(c_{21}))r^1_{12}r^2_{22}\cdots r^{n-1}_{22}=0$$

which implies that $(d_m(a_{11}+b_{12}+c_{21})-d_m(a_{11})-d_m(b_{12})-d_m(c_{21}))_{11}=0$. Consequently, $d_m(a_{11}+b_{12}+c_{21})-d_m(a_{11})-d_m(b_{12})-d_m(c_{21})=0$.

Similarly, we prove (ii). □

Lemma 2.9. *For any elements $a_{11}\in\mathscr{R}_{11}$, $b_{12}\in\mathscr{R}_{12}$, $c_{21}\in\mathscr{R}_{21}$ and $d_{22}\in\mathscr{R}_{22}$ holds $d_m(a_{11}+b_{12}+c_{21}+d_{22})=d_m(a_{11})+d_m(b_{12})+d_m(c_{21})+d_m(d_{22})$.*

Proof. For any elements $r^k_{i_kj_k}\in\mathscr{R}_{i_kj_k}$ $(k=1,\cdots,n-1)$ with $(i_1,j_1)=(1,1)$ and $(i_k,j_k)=(2,2)$ $(k=2,\cdots,n-1)$, or $(i_k,j_k)=(1,1)$ $(k=1,\cdots,n-1)$, or $(i_k,j_k)=(2,2)$ $(k=1,\cdots,n-1)$, we have by Lemma 2.8 that

$$\begin{aligned}
& d_m(r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots((a_{11}+b_{12}+c_{21}+d_{22})\circ r^1_{i_1j_1})\cdots))\\
= \;& d_m(r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots(a_{11}\circ r^1_{i_1j_1})\cdots))\\
& +d_m(r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots(b_{12}\circ r^1_{i_1j_1})\cdots))\\
& +d_m(r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots(c_{21}\circ r^1_{i_1j_1})\cdots))\\
& +d_m(r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots(d_{22}\circ r^1_{i_1j_1})\cdots))\\
= \;& r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots(d_m(a_{11})\circ r^1_{i_1j_1})\cdots)\\
& +\sum_{\substack{p_1+\ldots+p_n=m\\ p_2\neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}})\circ(\cdots(d_{p_k}(r^k_{i_kj_k})\\
& \qquad \circ(\cdots(d_{p_2}(a_{11})\circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots)\\
& +r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots(d_m(b_{12})\circ r^1_{i_1j_1})\cdots)\\
& +\sum_{\substack{p_1+\ldots+p_n=m\\ p_2\neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}})\circ(\cdots(d_{p_k}(r^k_{i_kj_k})\\
& \qquad \circ(\cdots(d_{p_2}(b_{12})\circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots)\\
& +r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots(d_m(c_{21})\circ r^1_{i_1j_1})\cdots)\\
& +\sum_{\substack{p_1+\ldots+p_n=m\\ p_2\neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}})\circ(\cdots(d_{p_k}(r^k_{i_kj_k})
\end{aligned}$$

$$\circ(\cdots(d_{p_2}(c_{21})\circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots)$$
$$+r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots(d_m(d_{22})\circ r^1_{i_1j_1})\cdots)$$
$$+\sum_{\substack{p_1+\ldots+p_n=m\\ p_2\neq m}} d_{p_n}(r^{n-1}_{i_{n-1}j_{n-1}})\circ(\cdots(d_{p_k}(r^k_{i_kj_k})$$
$$\circ(\cdots(d_{p_2}(d_{22})\circ d_{p_1}(r^1_{i_1j_1}))\cdots))\cdots). \tag{20}$$

Subtracting (2) from (20) it results that

$$r^{n-1}_{i_{n-1}j_{n-1}}\circ(\cdots((d_m(a_{11}+b_{12}+c_{21}+d_{22})$$
$$-d_m(a_{11})-d_m(b_{11})-d_m(c_{21})-d_m(d_{22}))\circ r^1_{i_1j_1})\cdots)=0. \tag{21}$$

As a consequence, if $(i_1,j_1)=(1,1)$ and $(i_k,j_k)=(2,2)$ $(k=2,\cdots,n-1)$, we get $(d_m(a_{11}+b_{12}+c_{21}+d_{22})-d_m(a_{11})-d_m(b_{12})-d_m(c_{21})-d_m(d_{22}))_{12}=0$ and $(d_m(a_{11}+b_{12}+c_{21}+d_{22})-d_m(a_{11})-d_m(b_{12})-d_m(c_{21})-d_m(d_{22}))_{21}=0$, by (21). If $(i_k,j_k)=(1,1)$ for all $(k=1,\cdots,n-1)$, then $(d_m(a_{11}+b_{12}+c_{21}+d_{22})-d_m(a_{11})-d_m(b_{12})-d_m(c_{21})-d_m(d_{22}))_{11}=0$, by (21) and [2, Lemma 2.1.(ii)]. If $(i_k,j_k)=(2,2)$ for all $(k=1,\cdots,n-1)$, we have $(d_m(a_{11}+b_{12}+c_{21}+d_{22})-d_m(a_{11})-d_m(b_{12})-d_m(c_{21})-d_m(d_{22}))_{22}=0$, by (21) and [2, Lemma 2.1.(ii)] again. It therefore follows that $d_m(a_{11}+b_{12}+c_{21}+d_{22})-d_m(a_{11})-d_m(b_{12})-d_m(c_{21})-d_m(d_{22})=0$. □

Lemma 2.10. *For any elements $a,b\in\mathscr{R}$ holds $d_m(a+b)=d_m(a)+d_m(b)$.*

Proof. The proof is a direct consequence of Lemmas 2.5, 2.6 and 2.9. Thus, d_m is additive. □

Now we are able to prove the Theorem 2.1.

Proof of Theorem 2.1. The Lemma 2.10 and the second principle of mathematical induction allows us to conclude that d_m is an additive map, for each non-negative integer m. Consequently, $D=\{d_m\}_{m\in\mathbb{N}}$ is a family of additive maps. The prove is complete. □

We may therefore state the following corollaries.

Corollary 2.1. *Let $\mathscr{R}$ be a ring 2 and $(2^{n-1}-1)$-torsion free prime ring containing a non-trivial idempotent e_1 and satisfying the following condition: $e_2r_1e_2 \circ (\cdots(e_2ae_2 \circ e_2r_1e_2)\cdots) = 0$, for all $r_1 \in \mathscr{R}$, implies $e_2ae_2 = 0$. Then every Jordan n-tuple higher derivable map $D = \{d_m\}_{m\in\mathbb{N}}$ is additive.*

As a direct consequence of the above Corollary 2.1 we have the following corollary.

Corollary 2.2. *Let $\mathscr{X}$ be a Banach space with $\dim \mathscr{X} > 1$ and $\mathscr{A} \subset \mathscr{B}(\mathscr{X})$ a standard operator algebra. Then every Jordan n-tuple higher derivable map $D = \{d_m\}_{m\in\mathbb{N}}$ is additive.*

Proof. Since it is well known that $\mathscr{A}$ is a prime ring of characteristic zero and containing a non-trivial idempotent, then it is sufficient to prove that the condition in Corollary 2.1 is satisfied. Hence, since $\mathscr{A}$ is dense in $\mathscr{B}(\mathscr{X})$ under the strong operator topology, let us consider a net $\{r_\lambda\}_{\lambda\in\Lambda} \subset \mathscr{B}(\mathscr{X})$ such that $SOT-\lim_\lambda r_\lambda = 1$. The limit in $e_2r_\lambda e_2 \circ (\cdots(e_2ae_2 \circ e_2r_\lambda e_2)\cdots) = 0$, for all $r_\lambda \in \mathscr{A}$, leads us to conclude that $e_2ae_2 = 0$. □

References

[1] M. Ashraf and N. Parveen, *Jordan higher derivable mappings on rings.* Algebra (2014). doi: 10.1155/2014/672387 (article ID 672387, 9 pages).

[2] J. C. M. Ferreira, M. G. B. Marietto and W. T. Botelho, *Additivity of Jordan n-tuple derivable maps on rings*, Algebras Groups Geom. 34, 13-30 (2017).

[3] W. Jing and F. Lu, *Additivity of Jordan (Triple) Derivations on Rings*, Comm. Algebra 40 (2012), 2700-2719.

ALGEBRAS GROUPS AND GEOMETRIES 35 347 - 364 (2018)
DOI 10.29083/AGG.35.04.2018

RINGS IN WHICH ELEMENTS ARE A SUM OF A CENTRAL AND NILPOTENT ELEMENT

Yosum Kurtlmaz
Department of Mathematics, Bilkent University
Ankara, Turkey
kurtulmazy@gmail.com

Abdullah Harmanci
Department of Mathematics, Hacettepe University
Ankara, Turkey
harmanci@hacettepe.edu.tr

Received May 24, 2020

Abstract

In this paper, we introduce a new class of rings whose elements are a sum of a central element and a nilpotent element, namely, a ring R is called CN if each element a of R has a decomposition $a = c + n$ where c is central and n is nilpotent. In this note, we characterize elements in $M_n(R)$ and $U_2(R)$ having CN-decompositions. For any field F, we give examples to show that $M_n(F)$ can not be a CN-ring. For a division ring D, we prove that if $M_n(D)$ is a CN-ring, then the cardinality of the center of D is strictly greater than n. Especially, we investigate several kinds of conditions under which some subrings of full matrix rings over CN rings are CN.
2010 AMS Mathematics Subject Classification: 15B33, 15B36, 16S70, 16U99.
Key words and phrases: CN ring, CN decomposition, matrix ring, uniquely nil clean ring, uniquely nil*-clean ring.

Copyright © 2018 by Hadronic Press Inc., Palm Harbor, FL 34682, U.S.A.

1 Introduction

Throughout this paper all rings are associative with identity unless otherwise stated. Let R be a ring. $\mathrm{Inv}(R)$, $J(R)$, $C(R)$ and $\mathrm{nil}(R)$ will denote the group of units, the Jacobson radical, the center and the set of all nilpotent elements of a ring R, respectively. Recall that in [2], uniquely nil clean rings are defined. An element a in a ring R is called *uniquely nil clean* if there is a unique idempotent $e \in R$ such that $a - e$ is nilpotent. The ring R is *uniquely nil clean* if each of its elements is uniquely clean. It is proved that in a uniquely nil clean ring, every idempotent is central. Also a uniquely nil clean ring R is called *uniquely strongly nil clean* [5] if a and e commute. Strongly nil cleanness and uniquely strongly nil cleanness are equivalent by [2]. Let R be a (*)-ring. In [7], $a \in R$ is called *uniquely strongly nil *-clean ring* if there is a unique projection $p \in R$, i.e., $p^2 = p = p^*$, and $n \in \mathrm{nil}(R)$ such that $a = p + n$ and $pn = np$. R is called a *uniquely strongly nil *-clean ring* if each of its elements is uniquely strongly nil *-clean. Another version of the notion of clean rings is that of CU rings. In [1], an element $a \in R$ is called a *CU element* if there exist $c \in C(R)$ and $n \in \mathrm{nil}(R)$ such that $a = c + n$. The ring R is called *CU* if each of its elements is CU. Motivated by these facts, we investigate basic properties of rings in which every element is the sum of a central element and a nilpotent element.

In what follows, $\mathbb{Z}_n$ is the ring of integers modulo n for some positive integer n. Let $M_n(R)$ denote the full matrix ring over R and $U_n(R)$ stand for the subring of $M_n(R)$ consisting of all $n \times n$ upper triangular matrices. And in the following, we give definitions of some other subrings of $U_n(R)$ to discuss in the sequel whether they satisfy CN property:

$$D_n(R) = \{(a_{ij}) \in M_n(R) \mid \text{ all diagonal entries of } (a_{ij}) \text{ are equal}\},$$

$$V_n(R) = \left\{ \sum_{i=j}^{n} \sum_{j=1}^{n} a_j e_{(i-j+1)i} \mid a_j \in R \right\},$$

$$V_n^k(R) = \left\{ \sum_{i=j}^{n} \sum_{j=1}^{k} x_j e_{(i-j+1)i} + \sum_{i=j}^{n-k} \sum_{j=1}^{n-k} a_{ij} e_{j(k+i)} : x_j, a_{ij} \in R \right\}$$

where $x_i \in R$, $a_{js} \in R$, $1 \leq i \leq k$, $1 \leq j \leq n-k$ and $k+1 \leq s \leq n$,

$$D_n^k(R) = \{\left\{\sum_{i=1}^{k}\sum_{j=k+1}^{n} a_{ij}e_{ij} + \sum_{j=k+2}^{n} b_{(k+1)j}e_{(k+1)j} + cI_n \mid a_{ij}, b_{ij}, c \in R\right\}$$

where $k = [n/2]$, i.e., k satisfies $n = 2k$ when n is an even integer, and $n = 2k+1$ when n is an odd integer, and

$$D_n^{\mathbb{Z}}(R) = \{(a_{ij}) \in U_n(R) \mid a_{11} = a_{nn} \in \mathbb{Z}, a_{ij} \in R, \{i,j\} \subseteq \{2,3,\ldots,n-1\}\}.$$

2 Basic Properties and Examples

Definition 2.1. Let R be a ring with identity. An element $a \in R$ is called *CN* or *it has a CN-decomposition* if $a = c + n$, where $c \in C(R)$ and $n \in \text{nil}(R)$. If every element of R has a CN decomposition, then R is called *a CN ring.*

We present some examples to illustrate the concept of CN property for rings.

Example 2.2. (1) Every commutative ring is CN.

(2) Every nilpotent element in a ring R has a CN decomposition.

(3) For a field F and for any positive integer n, $D_n(F)$ is a CN ring.

Proposition 2.3. *Let R be a ring and n a positive integer. Then $A \in M_n(R)$ has a CN decomposition if and only if for each $P \in GL_n(R)$, $PAP^{-1} \in M_n(R)$ has a CN decomposition.*

Proof. Assume that $A \in M_n(R)$ has a CN decomposition $A = C + N$ where $C \in C(M_n(R))$ and $N \in \text{nil}(M_n(R))$. Then $PAP^{-1} = PCP^{-1} + PNP^{-1}$ is a CN decomposition of PAP^{-1} since $PCP^{-1} = C \in C(M_n(R))$ and it is obvious that $PNP^{-1} \in \text{nil}(M_n(R))$. Conversely, suppose that PAP^{-1} has a CN decomposition $PAP^{-1} = C + N$. Then $A = P^{-1}CP + P^{-1}NP$ is the CN decomposition of PAP^{-1}. □

Let R be a commutative ring and n a positive integer. The following result gives us a way to find out whether $A \in M_n(R)$ has a CN decomposition. Note that it is easily shown that for a commutative ring $A \in C(M_n(R))$ if and only if $A = cI_n$ for some $c \in R$.

Theorem 2.4. *Let R be a commutative ring. Then $A \in M_n(R)$ has a CN decomposition if and only if $A - cI_n \in nil(M_n(R))$ for some $c \in R$.*

Proof. Assume that $A \in M_n(R)$ has a CN decomposition. By assumption there exists $c \in R$ such that $A - cI_n \in \text{nil}(M_n(R))$. Conversely, suppose that for any $A \in M_n(R)$, there exists $c \in R$ such that $A - cI_n \in \text{nil}(M_n(R))$. Since cI_n is central in $M_n(R)$, $A \in M_n(R)$ has a CN decomposition. □

Remark. Let R be a commutative ring. Then $A \in M_n(R)$ is a nilpotent matrix if and only if all eigenvalues of A are zero. A ring R is *reduced* if R has no nonzero nilpotent element. Hence we have.

Corollary 2.5. *Let R be a commutative reduced ring and n a positive integer. Then $A \in M_n(R)$ has a CN decomposition if and only if the only eigenvalue for $A - cI_n$ is 0 for some $c \in R$.*

Proposition 2.6. *Let R be a commutative ring. Then $U_2(R)$ is a CN ring if and only if for any $a, b \in R$, there exists $c \in R$ such that $a - c$, $b - c \in nil(R)$.*

Proof. Let $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \in M_2(R)$ has CN decomposition if and only if there exist $C = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} \in C(M_2(R))$ and $N = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \in \text{nil}(M_2(\mathbb{R}))$ such that $A = C + N$. Since $N \in \text{nil}(M_2(R))$ if and only if $x, z \in \text{nil}(R)$, $A = C + N$ is the CN decomposition of A if and only if there exists $c \in R$ such that $A - cI \in \text{nil}(M_2(R))$ if and only if $a - c$, $b - c \in \text{nil}(R)$. □

Example 2.7. Let $R = \mathbb{Z}$ and $A = \begin{bmatrix} 3 & 0 \\ 0 & 5 \end{bmatrix} \in U_2(R)$. Then there is no $c \in \mathbb{Z}$ such that $3 - c$ and $5 - c$ are nilpotent. By Proposition 2.6, $U_2(\mathbb{Z})$ is not CN.

Theorem 2.8. *Let R be a commutative local ring. If $M_2(R)$ is a CN ring, then $R/J(R)$ is not isomorphic to $\mathbb{Z}_2$.*

Proof. Assume that $M_2(R)$ is a CN ring. Suppose that $R/J(R)$ is isomorphic to $\mathbb{Z}_2$ and we get a contradiction. Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(R)$ and $f(c) = det(A - cI_2)$ be the characteristic polynomial of A. Then $f(c) = c(c-1) \in \text{nil}(R)$. By Proposition 2.6, $1-c$ and c are nilpotent. Since $1 = c + (1 - c)$, By hypothesis, c or $1 - c$ is invertible, therefore $c \in J(R)$ or $1 - c \in J(R)$. This is a contradiction. □

In [1], Chen and at al. defined and studied CU rings. Let R be a ring. An element $a \in R$ has a CU-decomposition if $a = c + u$ for some $c \in C(R)$ and $u \in U(R)$. A ring R is called CU, if every element of R has a CU-decomposition.

Proposition 2.9. *Every CN ring is CU.*

Proof. Let R be a CN ring and $a \in R$. By assumption $a + 1 = c + n$ for some $c \in C(R)$ and $n \in N(R)$. Hence $a = c+(n-1)$ is a CU decomposition of a. □

Theorem 2.10. *Let R be a division ring and n a positive integer. If $M_n(R)$ is a CN ring, then $|C(R)| > n$.*

Proof. Assume that $|C(R)| < n$. Consider A as a diagonal matrix which has the property that each element of $C(R)$ is one of the diagonal entries of A. For such a matrix A there is no $c \in C(R)$ for which $A - cI$ is a unit. Hence $M_n(R)$ is not a CU ring. By Proposition 2.9, $M_n(R)$ can not be a CN ring. This contradicts hypothesis. So $|C(R)| > n$. □

The converse of Proposition 2.9 is not true in general.

Example 2.11. Let $\mathbb{H} = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}\}$ be the ring of real quaternions, where $i^2 = j^2 = k^2 = ijk = 1$ and $ij = -ji, ik = -ki, jk = -kj$. $\mathbb{H}$ is a noncommutative division ring. Note that $C(\mathbb{H}) = \mathbb{R}$ and $nil(\mathbb{H}) = 0$. Let $a \in \mathbb{H}$. If $a = 0$, then $0 = 1 + (-1)$ is the CU-decomposition. If $a \neq 0$, then $a = 0 + a$ is the CU-decomposition of a. Hence $\mathbb{H}$ is a CU ring. On the other hand there is no CN decomposition of $i \in \mathbb{H}$. Hence it is not a CN ring.

Example 2.12. Let D be a division ring and consider the ring $D_2(D)$. The ring $D_2(D)$ is a noncommutative local ring, and so it is a CU-ring, but not a CN ring.

For a positive integer n, one may suspect that if R is a *CN* ring then the matrix ring $M_n(R)$ is also *CN*. The following examples shows that this is not true in general. Also whether or not $M_n(R)$ to be a CN ring does not depend on the cardinality of $C(R)$ comparing with n, that is, $|C(R)| \geq n$ or $|C(R)| < n$.

Example 2.13. (1) Since $\mathbb{Z}$ is commutative, it is a CN ring. But $R = M_2(\mathbb{Z})$ is not a CN ring.
(2) $R = M_2(\mathbb{Z}_3)$ is not a CN ring.
(3) $R = M_3(\mathbb{Z}_2)$ is not a CN ring.

Proof. (1) Consider $A = \begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix} \in M_2(\mathbb{Z})$ which is neither central nor nilpotent. Let $C = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} \in C(M_2(\mathbb{Z}))$ and $N = \begin{bmatrix} x & y \\ z & t \end{bmatrix} \in \text{nil}(M_2(\mathbb{Z}))$ with $A = C + N$. Then $x + t = 0$ and $zy = xt$. This is a contradiction. Hence A does not have CN decomposition.
(2) Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbb{Z}_3)$ which is neither central nor nilpotent. Assume that A has CN decomposition with $A = C + N$ where $C = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in C(M_2(\mathbb{Z}_3))$ and $N = \begin{bmatrix} x & y \\ t & u \end{bmatrix} \in \text{nil}(M_2(\mathbb{Z}_3))$. $A = C + N$ implies $1 = a + x$, $0 = a + u$ and $y = t = 0$. These equalities do not satisfied in $\mathbb{Z}_3$. For if $a = 0$, then $x = 1$; if $a = 1$, then $x = 0$ and $u = 2$; if $a = 2$, then $x = 2$ and $u = 1$. All these lead us a contradition. Hence $M_2(\mathbb{Z}_3)$ is not a CN ring.
(3) Let $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \in M_3(\mathbb{Z}_2)$ which is neither central nor nilpotent. Assume that A has CN decomposition with $A = C + N$ where $C = \begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix} \in C(M_3(\mathbb{Z}_2))$ and $N = \begin{bmatrix} x & y & z \\ t & u & v \\ k & l & m \end{bmatrix} \in \text{nil}(M_3(\mathbb{Z}_2))$. $A = C + N$

implies $1 = a + x$, $0 = a + u$, $0 = a + m$ and $y = z = v = t = k = l = 0$. These equalities do not satisfied in $\mathbb{Z}_2$. Hence $M_3(\mathbb{Z}_2)$ is not a CN ring. In fact, assume that $1 = a + x$ holds in $\mathbb{Z}_2$. There are two cases for a. $a = 0$ or $a = 1$. If $a = 1$ then $x = 0$ and $u = 1$. N being nilpotent implies $u = 1$ is nilpotent. A contradiction. Otherwise, $a = 0$. Then $x = 1$. Again N being nilpotent implies $x = 1$ is nilpotent. A contradiction. Thus $M_3(\mathbb{Z}_2)$ is not a CN ring. □

In spite of the fact that $U_n(R)$ need not be *CN* for any positive integer n, there are *CN* subrings of $U_n(R)$.

Proposition 2.14. *For a ring R and an integer $n \geq 1$, the following are equivalent:*
(1) *R is CN.*
(2) *$D_n(R)$ is CN.*
(3) *$D_n^k(R)$ is CN.*
(4) *$V_n(R)$ is CN.*
(5) *$V_n^k(R)$ is CN.*

Proof. Note that the elements of $D_n(R)$, $D_n^k(R)$, $V_n(R)$ and $V_n^k(R)$ having zero as diagonal entries are nilpotent. To complete the proof, it is enough to show (1) holds if and only if (2) holds for $n = 4$. The other cases are just a repetition.

(1) $\Rightarrow$ (2) Let $A = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ 0 & a_1 & a_5 & a_6 \\ 0 & 0 & a_1 & a_7 \\ 0 & 0 & 0 & a_1 \end{bmatrix} \in D_4(R)$. By (1), there exist $c \in C(R)$ and $n \in \text{nil}(R)$ such that $a_1 = c + n$.

Let $C = \begin{bmatrix} c & 0 & 0 & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & c \end{bmatrix}$ and $N = \begin{bmatrix} n & a_2 & a_3 & a_4 \\ 0 & n & a_5 & a_6 \\ 0 & 0 & n & a_7 \\ 0 & 0 & 0 & n \end{bmatrix}$. Then $C \in C(V_n(R))$ and $N \in \text{nil}(D_n(R))$.

(2) $\Rightarrow$ (1) Let $a \in R$. By (2) $A = \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{bmatrix} \in D_4(R)$ has a CN

decomposition $A = C + N$ where $C = \begin{bmatrix} c & 0 & 0 & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & c \end{bmatrix} \in C(D_4(R))$ and $N = \begin{bmatrix} n & * & * & * \\ 0 & n & * & * \\ 0 & 0 & n & * \\ 0 & 0 & 0 & n \end{bmatrix} \in C(D_n(R))$. Then $a = c + n$ with $c \in C(R)$ and $n \in \text{nil}(R)$. □

Lemma 2.15. *Every homomorphic image of CN ring is CN ring.*

Proof. Let $f : R \to S$ be an epimorphism of rings with R CN ring. Let $s = f(x) \in S$ with $x \in R$. There exist $c \in C(R)$ and $n \in \text{nil}(R)$ such that $x = c + n$. Since f is epic, $f(c) \in C(S)$ and $f(n) \in \text{nil}(R)$. Hence $s = f(c) + f(n)$ is CN decomposition of s. □

Proposition 2.16. *Let $R = \prod_{i \in I} R_i$ be a direct product of rings. R is CN if and only if R_i is CN for each $i \in I$.*

Proof. We may assume that $I = \{1, 2\}$ and $R = R_1 \times R_2$. Note that $C(R) = C(R_1) \times C(R_2)$ and $nil(R) = nil(R_1) \times nil(R_2)$.
Necessity: Let $r_1 \in R_1$. Then $(r_1, 0) = (c_1, c_2) + (n_1, n_2)$ where $(c_1, c_2) \in C(R)$ and $(n_1, n_2) \in nil(R)$. Hence $r_1 = c_1 + n_1$ is the CN decomposition of $r_1 \in R_1$. So R_1 is CN. A similar proof takes care for R_2 be CN.
Sufficiency: Assume that R_1 and R_2 are CN. Let $(r_1, r_2) \in R$. By assumption r_1 and r_2 have CN decompositions $r_1 = c_1 + n_1$ and $r_2 = c_2 + n_2$ where c_1 is central in R_1, n_1 is nilpotent in R_1 and c_2 is central in R_2, n_2 is nilpotent in R_2. Hence (r_1, r_2) has a CN decomposition $(r_1, r_2) = (c_1, c_2) + (n_1, n_2)$. This completes the proof. □

Let R be a ring and $D(\mathbb{Z}, R)$ denote the *Dorroh extension* of R by the ring of integers $\mathbb{Z}$ (see [3]). Then $D(\mathbb{Z}, R)$ is the ring defined by the direct sum $\mathbb{Z} \oplus R$ with componentwise addition and multiplication $(n, r)(m, s) = (nm, ns + mr + rs)$ where (n, r), $(m, s) \in D(\mathbb{Z}, R)$. It is clear that $C(D(\mathbb{Z}, R)) = \mathbb{Z} \oplus C(R)$. The identity of $D(\mathbb{Z}, R)$ is $(1, 0)$ and the set of all nilpotent elements is $\text{nil}(D(\mathbb{Z}, R)) = \{(0, r) \mid r \in \text{nil}(R)\}$.

Theorem 2.17. *Let R be a ring. Then R is a CN ring if and only if $D(\mathbb{Z}, R)$ is CN.*

Proof. Assume that R is CN. Let $(a, r) \in D(\mathbb{Z}, R)$. Since R is a CN ring, $r = c + n$ for some $c \in C(R)$ and $n \in \text{nil}(R)$. Then $(a, r) = (a, c) + (0, n)$ is the CN decomposition of (a, r). Conversely, let $r \in R$. Then $(0, r) = (a, c) + (0, s)$ as a CN decomposition where $(n, c) \in C(D(\mathbb{Z}, R))$ and $(0, n) \in \text{nil}(D(\mathbb{Z}, R))$. Then $c \in C(R)$ and $s \in \text{nil}(R)$. It follows that $r = c + s$ is the CN decomposition of r. Hence R is CN. □

Let R be a ring and S a subring of R and

$$T[R, S] = \{(r_1, r_2, \cdots, r_n, s, s, \cdots) : r_i \in R, s \in S, n \geq 1, 1 \leq i \leq n\}.$$

Then $T[R, S]$ is a ring under the componentwise addition and multiplication. Note that $\text{nil}(T[R, S]) = T[\text{nil}(R), \text{nil}(S)]$ and $C([T, S]) = T[C(R), C(R) \cap C(S)]$.

Proposition 2.18. *R be a ring and S a subring of R. Then the following are equivalent.*

1. *$T[R, S]$ is CN.*
2. *R and S are CN.*

Proof. (1) $\Rightarrow$ (2) Assume that $T[R, S]$ is a CN ring. Let $a \in R$ and $X = (a, 0, 0, \ldots) \in T[R, S]$. There exist a central element $C = (r_1, r_2, \cdots, r_n, s, s, \cdots)$ and a nilpotent element $N = (s_1, s_2, \cdots, s_k, t, t, \cdots)$ in $T[R, S]$ such that $X = C + N$. Then r_1 is in the center of R and s_1 is nilpotent in R and $a = r_1 + s_1$ is the CN decomposition of a. Hence R is CN. Let $s \in S$. By considering $Y = (0, s, s, s, \cdots) \in T[R, S]$, it can be seen that s has a CN decomposition.
(2) $\Rightarrow$ (1) Let R and S be CN rings and $Y = (a_1, a_2, \cdots, a_m, s, s, s, \cdots)$ be an arbitrary element in $T[R, S]$. Then there exist $c_i \in C(R)$, $1 \leq i \leq m$, $c \in C(R) \cap C(S)$ and $n_i \in \text{nil}(R)$, $1 \leq i \leq m$, $t \in \text{nil}(S)$ and such that $a_i = c_i + n_i$ for all $1 \leq i \leq m$ and $s = c + t$. Let $C = (c_1, c_2, \cdots, c_m, c, c, \cdots)$ and $N = (n_1, n_2, \cdots, n_m, t, t, \cdots)$. It is obvious that $C \in C(T[R, S])$ and $N \in \text{nil}(T[R, S])$. Hence $Y = C + N$ is a CN decomposition of Y. □

3 Some CN subrings of matrix rings

In this section, we study some subrings of full matrix rings whether or not they are CN rings. We first determine nilpotent and central elements of so-called subrings of matrix rings.

The rings $L_{(s,t)}(R)$ **:** Let R be a ring, and $s, t \in C(R)$. Let $L_{(s,t)}(R) = \left\{ \begin{bmatrix} a & 0 & 0 \\ sc & d & te \\ 0 & 0 & f \end{bmatrix} \in M_3(R) \mid a, c, d, e, f \in R \right\}$, where the operations are defined as those in $M_3(R)$. Then $L_{(s,t)}(R)$ is a subring of $M_3(R)$.

Lemma 3.1. *Let R be a ring, and let s, t be in the center of R. Then the following hold.*

(1) The set of all nilpotent elements of $L_{(s,t)}(R)$ is

$$nil(L_{(s,t)}(R)) = \left\{ \begin{bmatrix} a & 0 & 0 \\ sc & d & te \\ 0 & 0 & f \end{bmatrix} \in L_{(s,t)}(R) \mid a, d, f \in nil(R), c, e \in R \right\}.$$

(2) The set of all central elements of $L_{(s,t)}(R)$ is

$$C(L_{(s,t)}(R))) = \left\{ \begin{bmatrix} a & 0 & 0 \\ sc & d & te \\ 0 & 0 & f \end{bmatrix} \in H_{(s,t)}(R) \mid sa = sd, td = tf, a, d, f \in C(R) \right\}.$$

Proof. (1) Let $A = \begin{bmatrix} a & 0 & 0 \\ sc & d & te \\ 0 & 0 & f \end{bmatrix} \in \text{nil}(L_{(s,t)}(R)$. Assume that $A^n = 0$. Then $a^n = d^n = f^n = 0$. Conversely, Let $A = \begin{bmatrix} a & 0 & 0 \\ sc & d & te \\ 0 & 0 & f \end{bmatrix} \in (L_{(s,t)}(R)$ with $a^{n_1} = 0$, $d^{n_1} = 0$ and $f^{n_1} = 0$ and $n = \max\{n_1, n_2, n_3\}$. Then $A^{n+1} = 0$.
(2) Let $A = \begin{bmatrix} a & 0 & 0 \\ sc & d & te \\ 0 & 0 & f \end{bmatrix} \in C(L_{(s,t)}(R)))$ and $B = \begin{bmatrix} 1 & 0 & 0 \\ s & 0 & t \\ 0 & 0 & 0 \end{bmatrix} \in L_{(s,t)}(R))$.

By $AB = BA$ implies $sc + sd = sa$ and $td = tf$.....(*)
Let $C = \begin{bmatrix} 0 & 0 & 0 \\ s & 0 & t \\ 0 & 0 & 1 \end{bmatrix} \in L_{(s,t)}(R))$.
$AC = CA$ implies $sa = sd$ and $dt + te = tf$.....(**).
(*) and (**) implies $sa = sd$ and $tf = td$. For the converse inclusion,
let $A = \begin{bmatrix} a & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & f \end{bmatrix} \in L_{(s,t)}(R)$ with $sa = sd$, $td = tf$ and a, d, $f \in C(R)$.
Let $B = \begin{bmatrix} x & 0 & 0 \\ sy & z & tu \\ 0 & 0 & v \end{bmatrix} \in L_{(s,t)}(R)$. Then $AB = \begin{bmatrix} ax & 0 & 0 \\ sdy & dz & e \\ 0 & 0 & tdu \end{bmatrix}$, $BA = \begin{bmatrix} xa & 0 & 0 \\ sya & zd & tuf \\ 0 & 0 & vf \end{bmatrix}$. By the conditions; $sa = sd$, $td = tf$, $sc = 0$, $te = 0$ and a, d, $f \in C(R)$, $AB = BA$ for all $B \in L_{(s,t)}(R)$. Hence $A \in C(L_{(s,t)}(R))$. □

Consider following subrings of $L_{(s,t)}(R)$.

$$V_2(L_{(s,t)}(R)) = \left\{ \begin{bmatrix} a & 0 & 0 \\ 0 & a & te \\ 0 & 0 & a \end{bmatrix} \in L_{(s,t)}(R) \mid a, e \in R \right\}$$

$$C(L_{(s,t)}(R)) = \left\{ \begin{bmatrix} a & 0 & 0 \\ sc & d & te \\ 0 & 0 & f \end{bmatrix} \in L_{(s,t)}(R) \mid a, d, f \in C(R), c, e \in R, sa = sd, td = tf \right\}$$

It is easy to check that $V_2(L_{(s,t)}(R))$ and $C(L_{(s,t)}(R))$ are subrings of $L_{(s,t)}(R)$.

Proposition 3.2. *Let R be a ring. Following hold:*

(1) R is a CN ring if and only if $V_2(L_{(s,t)}(R))$ is a CN ring.

(2) $C(L_{(s,t)}(R))$ is a ring consisting of elements having CN decompositions.

(3) Assume that R is a CN ring. If for any $\{a, d, f\} \subseteq R$ having a CN decomposition $a = x+p$, $d = y+q$ and $f = z+r$ with $\{x, y, z\} \subseteq C(R)$ and $\{p, q, r\} \subseteq nil(R)$ satisfy $sx = sy$ and $ty = tz$, then $L_{(s,t)}(R)$ is a CN ring.

Proof. (1) Assume that R is a CN ring. Let $A = \begin{bmatrix} a & 0 & 0 \\ 0 & a & te \\ 0 & 0 & a \end{bmatrix} \in V_2(L_{(s,t)}(R))$. There exist $c \in C(R)$ and $n \in \text{nil}(R)$ such that $a = c + n$. Then $C = \begin{bmatrix} c & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c \end{bmatrix} \in C(L_{(s,t)}(R))$ and $N = \begin{bmatrix} n & 0 & 0 \\ 0 & n & te \\ 0 & 0 & n \end{bmatrix} \in \text{nil}(V_2(L_{(s,t)}(R)))$ and $A = C + N$ is the CN decomposition of A in $V_2(L_{(s,t)}(R))$. For the inverse implication, let $r \in R$ and consider $A = \begin{bmatrix} r & 0 & 0 \\ 0 & r & 0 \\ 0 & 0 & r \end{bmatrix} \in V_2(L_{(s,t)}(R))$. There exist $C = \begin{bmatrix} a & 0 & 0 \\ 0 & a & te \\ 0 & 0 & a \end{bmatrix} \in C(V_2(L_{(s,t)}(R)))$ and $N = \begin{bmatrix} p & 0 & 0 \\ 0 & r & tu \\ 0 & 0 & v \end{bmatrix} \in \text{nil}(V_2(L_{(s,t)}(R)))$. Then $a \in C(R)$ and $p \in \text{nil}(R)$ and $r = a + n$ is the CN decomposition of r. Hence R is a CN ring.

(2) Let $A = \begin{bmatrix} a & 0 & 0 \\ sc & d & te \\ 0 & 0 & f \end{bmatrix} \in CN_{(s,t)}(R)$. Set $C = \begin{bmatrix} a & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & f \end{bmatrix}$ and $N = \begin{bmatrix} 0 & 0 & 0 \\ sc & 0 & te \\ 0 & 0 & 0 \end{bmatrix}$. By Lemma 3.1, $C \in C(L_{(s,t)}(R))$ and $N \in \text{nil}(L_{(s,t)}(R)$. $A = C + N$ is the CN decomposition of A.

(3) Let $A = \begin{bmatrix} a & 0 & 0 \\ sc & d & te \\ 0 & 0 & f \end{bmatrix} \in L_{(s,t)}(R)$. Let $a = x+p$, $d = y+q$ and $f = z+r$ denote the CN decompositions of a, d and f. By hypothesis $sx = sy$ and $ty = tz$. By (2) A has a CN decomposition in $L_{(s,t)}(R)$ as $A = C+N$ where $C = \begin{bmatrix} x & 0 & 0 \\ 0 & y & 0 \\ 0 & 0 & z \end{bmatrix} \in C(L_{(s,t)}(R))$ and $N = \begin{bmatrix} p & 0 & 0 \\ sc & q & te \\ 0 & 0 & r \end{bmatrix} \in \text{nil}(L_{(s,t)}(R))$. □

Corollary 3.3. *Let R be a ring. If $L_{(s,t)}(R)$ is a CN ring, then R is a CN ring.*

Proof. Assume that $L_{(s,t)}(R)$ is a CN ring and let $a \in R$ and $A = \begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix} \in L_{(s,t)}(R)$. By hypothesis there exist $C = \begin{bmatrix} x & 0 & 0 \\ sy & z & tu \\ 0 & 0 & v \end{bmatrix} \in C(L_{(s,t)}(R))$ and $N = \begin{bmatrix} n & 0 & 0 \\ sc & m & te \\ 0 & 0 & k \end{bmatrix} \in \text{nil}(L_{(s,t)}(R))$ such that $A = C + N$ where $x \in C(R)$ and $n \in \text{nil}(R)$. Then $a = x + n$ is the CN decomposition of a. □

There are CN rings such that $L_{(s,t)}(R)$ need not be a CN ring.

Example 3.4. Let $R = \mathbb{Z}$ and $A = \begin{bmatrix} 1 & 0 & 0 \\ 3 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix} \in L_{(1,1)}(R)$. Assume that $A = C + N$ is a CN decomposition of A. Since A is neither central nor nilpotent, by Lemma 3.1, we should get A had a CN decomposition as $A = C + N$ where $C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in C(L_{(1,1)}(R))$ and $N = \begin{bmatrix} x & 0 & 0 \\ c & y & e \\ 0 & 0 & z \end{bmatrix} \in \text{nil}(L_{(1,1)}(R))$ where $\{x, y, z\} \subseteq \text{nil}(\mathbb{Z})$. This leads us a contradiction in $\mathbb{Z}$.

Proposition 3.5. *R is CN ring if and only if so is $L_{(0,0)}(R)$.*

Proof. Note that $L_{(0,0)}(R)$ is isomorphic to the ring $R \times R \times R$. By Proposition 2.16, $\prod_{i \in I} R_i$ is a CN ring if and only if each R_i is a CN ring for each $i \in I$. □

The rings $H_{(s,t)}(R)$: Let R be a ring and s, t be in the center of R. Let

$$H_{(s,t)}(R) = \left\{ \begin{bmatrix} a & 0 & 0 \\ c & d & e \\ 0 & 0 & f \end{bmatrix} \in M_3(R) \mid a, c, d, e, f \in R, a - d = sc, d - f = te \right\}.$$

Then $H_{(s,t)}(R)$ is a subring of $M_3(R)$. Note that any element A of $H_{(s,t)}(R)$ has the form $\begin{bmatrix} sc+te+f & 0 & 0 \\ c & te+f & e \\ 0 & 0 & f \end{bmatrix}$.

Lemma 3.6. *Let R be a ring, and let s,t be in the center of R. Then the set of all nilpotent elements of $H_{(s,t)}(R)$ is*

$$nil(H_{(s,t)}(R)) = \left\{ \begin{bmatrix} a & 0 & 0 \\ c & d & e \\ 0 & 0 & f \end{bmatrix} \in H_{(s,t)}(R) \mid a,d,f \in nil(R), c,e \in R \right\}.$$

Proof. Let $A = \begin{bmatrix} a & 0 & 0 \\ c & d & e \\ 0 & 0 & f \end{bmatrix} \in \text{nil}(H_{(s,t)}(R))$. There exists a positive integer n such that $A^n = 0$. Then $a^n = d^n = f^n = 0$. Conversely assume that $a^n = 0$, $d^m = 0$ and $f^k = 0$ for some positive integers n, m, k. Let $p = max\{n, m, k\}$. Then $A^{2p} = 0$. □

Lemma 3.7. *Let R be a ring, and let s and t be central invertible in R. Then*

$$C(H_{(s,t)}(R)) = \left\{ \begin{bmatrix} a & 0 & 0 \\ c & d & e \\ 0 & 0 & f \end{bmatrix} \in H_{(s,t)}(R) \mid c,e,f \in C(R) \right\}.$$

Proof. [4, Lemma 3.1]. □

Theorem 3.8. *Let R be a ring. R is a CN ring if and only if $H_{(s,t)}(R)$ is a CN ring.*

Proof. Assume that R is a CN ring. Let $A = \begin{bmatrix} a & 0 & 0 \\ c & d & e \\ 0 & 0 & f \end{bmatrix} \in (H_{(s,t)}(R))$. Then $a = c_1 + n_1$, $d = c_2 + n_2$, $f = c_3 + n_3$, $c = c_4 + n_4$, $e = c_5 + n_5$ with $\{c_1, c_2, c_3, c_4, c_5\} \subseteq C(R)$, $\{n_1, n_2, n_3, n_4, n_5\} \subseteq \text{nil}(R)$. Let $c_1 - c_2 = sc_4$, $c_2 - c_3 = tc_5$, $n_1 - n_2 = sn_4$ and $n_2 - n_3 = tn_5$ and $C = \begin{bmatrix} c_1 & 0 & 0 \\ c_4 & c_2 & c_5 \\ 0 & 0 & c_3 \end{bmatrix}$ and

$N = \begin{bmatrix} n_1 & 0 & 0 \\ n_4 & n_2 & n_5 \\ 0 & 0 & n_3 \end{bmatrix}$. By Lemma 3.7, $C \in C(H_{(s,t)}(R))$ and by Lemma 3.6, $N \in \text{nil}(H_{(s,t)}(R))$. Then $A = C + N$ is the CN decomposition of A.

Conversely, suppose that $H_{(s,t)}(R)$ is a CN ring. Let $a \in R$. Then $A = \begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix} \in (H_{(s,t)}(R))$ and it has a CN decomposition $A = C + N$ where $C = \begin{bmatrix} x & 0 & 0 \\ y & z & u \\ 0 & 0 & v \end{bmatrix} \in C(H_{(s,t)}(R))$ with $\{y, u, v\} \subseteq C(R)$ and $N = \begin{bmatrix} n_1 & 0 & 0 \\ n_2 & n_3 & n_4 \\ 0 & 0 & n_5 \end{bmatrix} \in \text{nil}(H_{(s,t)}(R))$ with $\{n_1, n_3, n_5\} \subseteq \text{nil}(R)$. Then $a = x + n_1$ is a CN decomposition of a. □

Proposition 3.9. *Uniquely nil clean rings, uniquely strongly nil clean rings, strongly nil *-clean rings are CN.*

Proof. These classes of rings are abelian. Assume that R is uniquely nil clean ring. Let e be an idempotent in R. For any $r \in R$, $e + (re - ere)$ can be written in two ways as a sum of an idempotent and a nilpotent as $e+(re-ere) = (e+(re-ere))+0 = e+(re-ere)$. Then $e = e+(re-ere)$ and $er - ere = 0$. Similarly, $e+(er-ere) = (e+(re-ere))+0 = e+(er-ere)$. Then $0 = re - ere \simeq re - ere$. Hence e is central. □

The converse of this result is not true.

Example 3.10. *The ring $H_{(0,0)}(\mathbb{Z})$ is CN but not uniquely nil clean.*

Proof. By Theorem 3.8, $H_{(0,0)}(\mathbb{Z})$ is CN. Note that for $n \in \mathbb{Z}$ has a uniquely nil clean decomposition if and only if $n = 0$ or $n = 1$. Let $A = \begin{bmatrix} a & 0 & 0 \\ c & a & e \\ 0 & 0 & a \end{bmatrix} \in H_{(0,0)}(R)$ with $a \notin \{0, 1\}$. Assume that A has a uniquely nil clean decomposition. There exist unique $E^2 = E = \begin{bmatrix} x & 0 & 0 \\ y & x & u \\ 0 & 0 & x \end{bmatrix} \in H_{(0,0)}(R)$ and

$N = \begin{bmatrix} g & 0 & 0 \\ h & g & l \\ 0 & 0 & g \end{bmatrix} \in N(H_{(0,0)}(R)$ such that $A = E + N$. Then A has a uniquely nil clean decomposition. So $a = x + g$ has a CN decomposition. This is not the case for $a \in \mathbb{Z}$. Hence $H_{(0,0)}(\mathbb{Z})$ is not uniquely nil clean. □

Generalized matrix rings: Let R be ring and s a central element of R. Then $\begin{bmatrix} R & R \\ R & R \end{bmatrix}$ becomes a ring denoted by $K_s(R)$ with addition defined componentwise and with multiplication defined in [6] by

$$\begin{bmatrix} a_1 & x_1 \\ y_1 & b_1 \end{bmatrix} \begin{bmatrix} a_2 & x_2 \\ y_2 & b_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + sx_1y_2 & a_1x_2 + x_1b_2 \\ y_1a_2 + b_1y_2 & sy_1x_2 + b_1b_2 \end{bmatrix}.$$

In [6], $K_s(R)$ is called a *generalized matrix ring over* R.

Lemma 3.11. *Let R be a commutative ring. Then the following hold.*

(1) $nil(K_0(R)) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in K_0(R) \mid \{a, d\} \subseteq nil(R) \right\}$.

(2) $C(K_0(R))$ consists of all scalar matrices.

Proof. (1) Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{nil}(K_0(R))$. Then $A^2 = \begin{bmatrix} a^2 & b(a+d) \\ c(a+d) & d^2 \end{bmatrix}$, ..., ..., $A^{2^n} = \begin{bmatrix} a^{2^n} & \Sigma_{i=1}^{n} b(a^{2^{i-1}} + d^{2^{i-1}}) \\ \Sigma_{i=1}^{n} c(a^{2^{i-1}} + d^{2^{i-1}}) & d^{2^n} \end{bmatrix}$. Hence $A \in \text{nil}(K_0(R))$ if and only if $\{a, d\} \subseteq \text{nil}(R)$. □

Lemma 3.12. *Let R be ring. Then R is a CN ring if and only if $D_n(K_0(R))$ is a CN ring.*

Proof. Necessity: We assume that $n = 2$. Let $A = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \in D_2((K_0(R)))$. By assumption $a = c_1 + n_1$ where $c_1 \in C(R)$ and $n_1 \in \text{nil}(R)$. Let $C = \begin{bmatrix} c_1 & 0 \\ 0 & c_1 \end{bmatrix} \in C(D_2(K_0(R)))$ and $N = \begin{bmatrix} n_1 & b \\ 0 & n_1 \end{bmatrix} \in \text{nil}D_2((K_0(R)))$. $A = C+N$ is the CN decomposition of A.

Sufficiency: Let $a \in R$. Then $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in D_2((K_0(R)))$ has a CN decomposition $A = C + N$ with $C = \begin{bmatrix} c_1 & 0 \\ 0 & c_1 \end{bmatrix} \in C(D_2((K_0(R))))$ and $N = \begin{bmatrix} n_1 & b_1 \\ 0 & n_1 \end{bmatrix} \in \text{nil}(D_2((K_0(R))))$ where $c_1 \in C(R)$ and $n_1 \in \text{nil}(R)$. By comparing components of matrices we get $a = c_1 + n_1$. It is a CN decomposition of a. □

Note that $K_0(R)$ need not be a CN ring.

Example 3.13. Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in K_0(\mathbb{Z})$ have a CN decomposition as $A = C + N$ where $C \in C(K_0(\mathbb{Z}))$ and $N \in \text{nil}K_0(\mathbb{Z}))$. Then we should have $C = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}$ and $N = \begin{bmatrix} 1-x & 0 \\ 0 & -x \end{bmatrix}$. These imply $x = 1$ or x is nilpotent. A contradiction.

References

[1] H. Chen, S. Halicioglu, A. Harmanci and Y. Kurtulmaz, *On the Decomposition of a Matrix into the Sum of a Central Matrix and a Unit Matrix* , submitted for publication.

[2] A. J. Diesl, *Nil clean rings*, J. Algebra, 383(2013), 197-211.

[3] J. L. Dorroh, *Concerning Adjunctions to Algebras*, Bull. Amer. Math. Soc., 38(1932), 85-88.

[4] H. Kose, Y. Kurtulmaz, B. Ungor and A. Harmanci, *Rings Having Normality in terms of the Jacobson Radical*, Arab. J. Math., https://doi.org/10.1007/s40065-018-0231-7.

[5] Y. Hirano, H. Tominaga and A. Yaqub, *On rings in which every element is uniquely expressable as a sum of a nilpotent element and a certain potent element*, Math. J. Okayama Univ. 30(1988), 33-40.

[6] P. A. Krylov, *Isomorpism of generalized matrix rings*, Algebra and Logic, 47(4)(2008), 258-262.

[7] C. Li and Y. Zhou, *On strongly *-clean rings*, J. Algebra Appl. 10(2011), 1363-1370.

ALGEBRAS GROUPS AND GEOMETRIES 35 365 - 388 (2018)
DOI 10.29083/AGG.35.04.2018

HAMILTON-JACOBI TREATMENT OF SUPERSTRING AND QUANTIZATION OF FIELDS WITH CONSTRAINTS

W. I. Eshraim
Institute for Theoretical Physics, Goethe University, Frankfurt am Main,
Institute for Theoretical Physics, Justus-Liebig University,
Giessen, Germany
weshraim@th.physik.uni-frankfurt.de

Received March 2, 2020
Revised April 29, 2020

Abstract

The Hamilton-Jacobi formalism of constrained systems is used to study superstring. That obtained the equations of motion for a singular system as total differential equations in many variables. These equations of motion are in exact agreement with those equations obtained using Dirac's method. Moreover, the Hamilton-Jacobi quantization of a constrained system is discussed. Quantization of the relativistic local free field with linear velocity of dimension D containing second-class constraints is studied. The set of Hamilton-Jacobi partial differential equations and the path integral of these theories are obtained by using the canonical path integral quantization. We figured out that the Hamilton-Jacobi path integral quantization of this system is in exact agreement with that given by using Senjanovic method. Furthermore, Hamilton-Jacobi path integral quantization of the scalar field coupled to two flavours of fermions through Yukawa couplings is obtained directly as an integration over the canonical phase space. Hamilton-Jacobi quantization is applied to the constraint field systems with finite degrees of freedom by investigating the integrability conditions without using any gauge fixing condition.

keywords: Field Theory; Gauge Fields; Hamilton-Jacobi Formulation; Singular Lagrangian, Path Integral Quantization of Constrained Systems.

Copyright © 2018 by Hadronic Press Inc., Palm Harbor, FL 34682, U.S.A.

1 Introduction

The generalized Hamiltonian dynamics describing systems with constraints was initiated by Dirac [1, 2], who established a formalism for treating constraint singular systems. The presence of constraints in such theories requires care when applying Dirac's method, especially when first-class constraints arise since the first-class constraints are generators of gauge transformations which lead to the gauge freedom. Dirac showed that the algebra of Poisson brackets determines a division of constraints into two classes: so-called first-class and second-class constraints. The first-class constraints are those that have zero Poisson brackets with all other constraints in the subspace of phase space in which constraints hold; constraints which are by definition second-class. Most physicists believe that this distinction is quite important not only in classical theories but also in quantum mechanics [3, 4].

As a first step in the present work, we intend to study a singular system with Lagrangian describing superstring from the point of view of the Hamilton-Jacobi formalism which has been developed by Güler [5, 6] to investigate constrained systems. The equivalent Lagrangian method [7] is used to obtain the set of Hamilton-Jacobi partial differential equations (HJPDE). The study of such systems through Dirac's generalized Hamiltonian formalism has already been extensively developed in literature [3, 4] to investigate theoretical models in contemporary elementary particle physics and will be used here for comparative purposes.

Despite the success of Dirac's approach in studying singular systems, which is demonstrated by the wide number of physical systems to which this formalism has been applied, it is instructive to study singular systems through other formalisms, since different procedures will provide different views for the same problems, even for nonsingular systems. The Hamilton-Jacobi approach that we study in this work, is applied to some physical examples [8, 9, 10, 11, 12, 13]. But it is still lacking to a better understanding of this approach utility in the studying singular systems, and such understanding can only be achieved through its application to other interesting physical systems. From our aims in this work is to treat the superstring constraint system by the Hamilton-Jacobi approach and compare the results to those obtained through Dirac's method.

In the case of unconstrained systems, the Hamilton-Jacobi theory pro-

vides a bridge between classical and quantum mechanics. The first study of the Hamilton-Jacobi equations for arbitrary first-order actions was initiated by Santilli [14]. The quantization and construction of functional integral for theories with first-class constraints in canonical gauge was given by Faddeev and Popov [15, 16]. Faddeev's method is generalized by Senjanovic [17] to the case of appearance of the second-class constraints in the theory. Moreover, Fradkin [18] considered quantization of bosonic theories with first- and second-class constraints and the extension to include in such gauges. Gitman and Tyutin [3] discussed the Hamiltonian formalism of gauge theories in an arbitrary gauge and the canonical quantization of singular theories. In the Hamiltonian-Jacobi approach, the distinction between first- and second-class constraints is not necessary. The equations of motion are written as total differential equations in many variables, which need to investigate the integrability conditions. In other words, the integrability conditions may lead to new constraints. Moreover, it is shown that gauge fixing, which is a basic procedure to study singular systems by Dirac's method, is not necessary if the canonical method is used [7]. The path integral formulation based on the canonical method is obtained in Refs. [19, 20, 21, 22].

In Ref. [23], We have studied successfully the first-class constraints in canonical gauge by applying the Faddeev and Hamilton-Jacobi methods to obtain the path integral quantization of the scalar field coupled minimally to the vector potential. That led to the same results by the two methods which prove that the Hamilton-Jacobi method apple to quantized the first-class constraints. For more complement of confirmation the successful of Hamilton-Jacobi method, we quantize the relativistic local free field with a linear velocity of dimension D with the second-class constraints. The path integral quantization of this field is obtained by using the Senjanovic and Hamilton-Jacobi methods. We noticed that Faddeev [23], Popov and Senjanovic treatment need gauge-fixing conditions to obtain the path integral over the canonical variable, which is not always an easy task. However, if the Hamilton-Jacobi approach [5, 6] is used, the gauge fixing is not necessary to analyze singular systems [9]. From the previous comparison, we figure out the ability and simplicity of using the Hamilton-Jacobi approach for studying the constraint systems. So, in the end, we get the path integral quantization of the scalar field coupled to two flavours of fermions through Yukawa couplings by using Hamilton-Jacobi quantization.

2 Hamilton-Jacobi Approach

In this section, we approach the constrained systems by Hamilton-Jacobi treatment, which solves the gauge-fixing problem naturally.
Güler [5, 6] has developed a completely different method to investigate singular systems. He started with the Hess matrix elements A_{ik} of second derivatives of the Lagrangian $\mathcal{L} = \mathcal{L}(\varphi_i,\, \partial\varphi_i,\, \tau\,)$, $i = 1, ..., n$, which defined as

$$A_{ik} = \frac{\delta^2 \mathcal{L}(\varphi_i,\, \partial\varphi_i,\, \tau\,)}{\delta(\partial\varphi_i)\delta(\partial\varphi_k)}\,, \qquad i,k = 1,2,...,n\,, \tag{1}$$

of rank $(n-r)$, $r < n$, with dependent momenta r. The equivalent Lagrangian method [7] is used to obtain the set of Hamilton-Jacobi Partial Differential Equations (HJPDE). The generalized momenta corresponding to generalized coordinates φ_i are defined as

$$\pi_a = \frac{\overrightarrow{\delta}\mathcal{L}}{\delta(\partial_\mu\varphi_a)}, \qquad a = 1,2,\ldots,n-r\,, \tag{2}$$

$$\pi_j = \frac{\overrightarrow{\delta}\mathcal{L}}{\delta(\partial_\mu\varphi_j)}, \qquad j = n-r+1,\ldots,n\,, \tag{3}$$

where φ_i are divided into two sets φ_a and x_j. Since the rank of Hess matrix is $(n-r)$, one may solve Eq.(2) for $\partial_\mu\varphi_a$ as

$$\partial_\mu\varphi_a = \partial_\mu\varphi_a(\varphi_i, \pi_a, \partial_\mu\varphi_j; \chi_\mu) \equiv \omega_a\,, \tag{4}$$

By substituting Eq. (4) into Eq. (3), we get

$$\pi_j = \left.\frac{\overrightarrow{\delta}\mathcal{L}}{\delta(\partial_\mu\varphi_j)}\right|_{\partial_\mu\varphi_a=\omega_a} \equiv -\mathcal{H}_j(\varphi_i, \partial_\mu\varphi_\nu, \pi_a; \chi_\mu)\,, \tag{5}$$

which indicate to the fact that the generalized momenta π_j depend on π_a. That is a normal result of the singular nature of the Lagrangian.
The canonical Hamiltonian $\mathcal{H}_0$ is given by the following definition

$$\mathcal{H}_0 = -\mathcal{L}(\varphi_i, \partial_\mu\varphi_\nu, \partial_\mu\varphi_a \equiv \omega_a, \chi_\mu) + \pi_a\omega_a + \pi_j\partial_\mu\varphi_j\big|_{\pi_\nu=-\mathcal{H}_\nu}\,. \tag{6}$$

The expression of the set of Hamilton-Jacobi Partial Differential Equations (HJPDE) is

$$\mathcal{H}_0'\left(\tau,\ \varphi_\nu,\ \varphi_a,\ \pi_i = \frac{\overrightarrow{\delta}S}{\delta\varphi_i},\ \pi_0 = \frac{\overrightarrow{\delta}S}{\delta\chi_\mu}\right) = 0, \tag{7}$$

$$\mathcal{H}'_\mu\left(\tau,\ \varphi_\nu,\ \varphi_a,\ \pi_i=\frac{\overrightarrow{\delta}S}{\delta\varphi_i},\ \pi_0=\frac{\overrightarrow{\delta}S}{\delta\chi_\mu}\right)=0, \tag{8}$$

where S being the action.
Eqs. (7) and (8) may be expressed in a compact form as

$$\mathcal{H}'_\alpha\left(\tau,\ \varphi_\nu,\ \varphi_a,\ \pi_i=\frac{\overrightarrow{\delta}S}{\delta\varphi_i},\ \pi_0=\frac{\overrightarrow{\delta}S}{\delta\chi_\alpha}\right)=0, \tag{9}$$

$$\alpha=0,n-r+1,\ldots,n\,.$$

where

$$\mathcal{H}'_0=\pi_0+\mathcal{H}_0=0\,, \tag{10}$$
$$\mathcal{H}'_\mu=\pi_j+\mathcal{H}_j=0\,. \tag{11}$$

Here $\mathcal{H}'_0$ can be interpreted as the generator of time evolution while $\mathcal{H}'_j$ are the generators of gauge transformation.
The fundamental equations of the equivalent Lagrangian method are

$$\pi_0=\frac{\overrightarrow{\delta}S}{\overrightarrow{\delta}\chi_\mu}\equiv-\mathcal{H}_0(\varphi_i,\delta_\mu\varphi_\nu,\pi_a;\chi_\mu)\,, \tag{12}$$

$$\pi_a=\frac{\overrightarrow{\delta}S}{\delta\varphi_a},\qquad \pi_j=\frac{\overrightarrow{\delta}S}{\delta\varphi_j}\equiv-\mathcal{H}_j\,, \tag{13}$$

with $\varphi_0=\chi_\mu$. That gives the equations of motion as total differential equations in many variables as

$$d\varphi_r=\frac{\overrightarrow{\delta}\mathcal{H}'_\alpha}{\delta\pi_r}\,d\chi_\alpha,\qquad r=0,1,\ldots,n\,, \tag{14}$$

$$d\pi_a=-\frac{\overrightarrow{\delta}\mathcal{H}'_\alpha}{\delta\varphi_a}\,d\chi_\alpha,\qquad a=1,\ldots,n-r\,, \tag{15}$$

$$d\pi_\mu=-\frac{\overrightarrow{\delta}\mathcal{H}'_\alpha}{\delta\varphi_\mu}\,d\chi_\alpha,\qquad \mu=n-r+1,\ldots,n\,, \tag{16}$$

$$dZ=\left(-\mathcal{H}_\alpha+\pi_a\frac{\overrightarrow{\delta}\mathcal{H}'_\alpha}{\delta\pi_a}\right)d\chi_\alpha,\quad \alpha=0,n-r+1,\ldots,n\,, \tag{17}$$

where $Z = S(\chi_\alpha, \varphi_a)$. These equations are integrable if and only if

$$d\mathcal{H}'_0 = 0\,, \tag{18}$$

$$d\mathcal{H}'_\beta = 0, \qquad \beta = 1, 2, \ldots, r\,. \tag{19}$$

In the case of not satisfied the conditions (18) and (19) identically, one has to consider them as new constraints and then we examine again the variations of them. One is repeating this procedure until obtain a set of conditions with all variations vanish.

The investigation of the integrability conditions [24, 25] can be also done by using the operator method, where the linear operators X_α corresponding to the set (14 - 16) are defined as

$$X_\alpha f(\chi_\beta, \varphi_a, \pi_a, z) = \frac{\delta f}{\delta \chi_\alpha} + \frac{\delta \mathcal{H}'_\alpha}{\delta \pi_a}\,\frac{\delta f}{\delta \varphi_a} - \frac{\delta \mathcal{H}'_\alpha}{\delta \varphi_a}\,\frac{\delta f}{\delta \pi_a} + \left(-\mathcal{H}_\alpha + \pi_a \frac{\delta \mathcal{H}'_\alpha}{\delta \pi_a}\right)\frac{\delta f}{\delta z}\,. \tag{20}$$

The system is integrable, if the bracket relations

$$[X_\alpha, X_\beta] f = (X_\alpha X_\beta - X_\beta X_\alpha) f = C^\gamma_{\alpha\beta} X_\gamma f; \quad \forall\ \alpha, \beta, \gamma = 0, n-r+1, \ldots, n\,, \tag{21}$$

are hold. If the relations (14 - 16) are not satisfied identically, we add the bracket relations, which cannot be expressed in this form as new operators. So the numbers of independent operators are increased, and a new complete system can be obtained. Then the new operators can be written in the Jacobi form, and we fined the corresponding integrable system of the total differential equations.

3 Path Integral Quantization

In this section, we briefly review the Senjanovic's and Hamilton-Jacobi methods for studying the path integral quantization of constrained systems.

3.1 Senjanovic Method

We generalize Faddeeve's method [15] to the case when second-class constraints are present. This generalization is called Senjanovic's method.
Consider a mechanical system with α first-class constraints ϕ_a, β second-class constraints θ_b, and the gauge conditions associated with the first-class

constraints χ_a. Let the χ_a be chosen in such a way that $\{\chi_a, \chi_b\} = 0$. Then the expression for the S-matrix element is [17]

$$\langle Out \mid S \mid In \rangle = \int exp\left[i \int_{-\infty}^{\infty} (p_i \dot{q}_i - H_0)\, dt\right] \prod_t d\mu(q(t), p(t))\,, \qquad (22)$$

and

$$d\mu(q,p) = \left(\prod_{a=1}^{\alpha} \delta(\chi_a)\delta(\phi_a)\right) det||\{\chi_a, \phi_a\}|| \times \prod_{b=1}^{\beta} \delta(\theta_b)\, det||\{\theta_a, \theta_b\}||^{\frac{1}{2}} \prod_{i=1}^{n} dp_i\, dq^i\,. \qquad (23)$$

where H_0 is the Hamiltonian of the system and $d\mu(q,p)$ is the measure of integration.

3.2 Hamilton-Jacobi Quantization

In Refs. [19, 20, 21, 23, 24, 25, 26], the path integral formulation of the constrained systems is studied. For computing the Hamilton-Jacobi path integral, one has to consider a singular Lagrangian as seen in section II. The canonical Hamiltonian H_0 defined in Eq. (6), and the set of HJPDE is expressed in Eqs. (7) and (8). As we define $p_\beta = \frac{\partial S[q_a; x_\alpha]}{\partial x_\beta}$ and $p_a = \frac{\partial S[q_a; x_\alpha]}{\partial q_a}$ with $x_0 = t$ and S being the action. The total differential equations given in (14 - 17) are integrable if (18) and (19) are hold [26]. If conditions (18) and (19) are not satisfied identically, one considers them as new constraints and again consider their variations.

Thus, repeating this procedure one may obtain a set of constraints such that all variations vanish. Simultaneous solutions of canonical equations with all these constraints provide to obtain the set of canonical phase space coordinates (q_a, p_a) as functions of t_α, besides the canonical action integral is obtained in terms of the canonical coordinates. H'_α can be interpreted as the infinitesimal generator of canonical transformations given by parameters

t_α. In this case path integral representation may be written as

$$\langle Out \mid S \mid In\rangle = \int \prod_{a=1}^{n-p} dq^a dp^a exp\left\{\int_{t_\alpha}^{t'_\alpha}\left(-H_\alpha + p_\alpha \frac{\partial H'_\alpha}{\partial p_\alpha}\right) dt_\alpha\right\},$$
$$a = 1,\ldots,n-p, \qquad \alpha = 0, n-p+1,\ldots,n\,. \quad (24)$$

In fact, this path integral is an integration over the canonical phase-space coordinates (q^a, p^a).

4 Hamilton-Jacobi treatment of superstring

In this section we treat supersting constraint system by Dirac's method and then apply Hamilton-Jacobi method.

4.1 Dirac's formulation of superstring

Consider a Lagrangian describes a superstring system

$$L = -\frac{1}{2\pi}\left(\partial_\alpha X^\mu \partial^\alpha X_\mu - i\,\overline{\psi}^{\,\mu}\rho^\alpha \partial_\alpha \psi_\mu\right) - \jmath^\alpha A_\alpha - \frac{1}{4\pi}F^{\alpha\beta}F_{\alpha\beta}\,, \quad (25)$$

Where A^α is a world sheet potential analogous to the electromagnetic potential. The world sheet current density

$$\jmath_\alpha = \frac{1}{2\pi}\, q\,\overline{\psi}^{\,\mu}\rho^\alpha \psi_\mu\,, \quad (26)$$

acts as a source for the gauge field (A^α), and the electromagnetic tensor is defined as $F^{\alpha\beta} = \partial^\alpha A^\beta - \partial^\beta A^\alpha$.

The Lagrangian (25) is singular, since the rank of the Hess matrix (1) is four. The generalized momenta (2) and (3) can be written as

$$p_\mu = \frac{\partial L}{\partial \dot{X}^\mu} = -\frac{1}{\pi}\,\partial^0 X_\mu\,, \quad (27)$$

$$p^\mu_{\overline{\psi}} = \frac{\partial L}{\partial \dot{\overline{\psi}}^{\,\mu}} = 0 = -H_{\overline{\psi}}\,, \quad (28)$$

$$p^\mu_\psi = \frac{\partial L}{\partial \dot{\psi}_\mu} = \frac{i}{2\pi}\overline{\psi}^{\,\mu}\rho^0 = -H_\psi\,, \quad (29)$$

$$\pi^i = \frac{\partial L}{\partial \dot{A}_i} = \frac{1}{\pi} F^{i0}\,, \tag{30}$$

$$\pi^0 = \frac{\partial L}{\partial \dot{A}_0} = 0 = -H_1\,. \tag{31}$$

Equations (27) and (30), respectively leads us to express the velocities $\dot{X}^\mu$ and $\dot{A}_i$ as

$$\dot{X}^\mu = -\pi\, p^\mu\,, \tag{32}$$

$$\dot{A}_i = -\pi\, \pi_i + \partial_i A_0\,. \tag{33}$$

The Hamiltonian density is given by

$$\begin{aligned} H_0 = &-\frac{\pi}{2}(p^\mu\, p_\mu + \pi^i\, \pi_i) + \pi^i\, \partial_i A_0 \\ &+ \frac{1}{2\pi}[\partial_i X^\mu\, \partial^i X_\mu - i\overline{\psi}^{\,\mu} \rho^i\, \partial_i \psi_\mu + q\overline{\psi}^{\,\mu} \rho^\alpha \psi_\mu A_\alpha + \frac{1}{2} F^{ij}\, F_{ij}]\,. \end{aligned} \tag{34}$$

The total Hamiltonian density is constructed as

$$\begin{aligned} H_T = &-\frac{\pi}{2}(p^\mu\, p_\mu + \pi^i\, \pi_i) + \pi^i\, \partial_i A_0 + \frac{1}{2\pi}[\partial_i X^\mu\, \partial^i X_\mu - i\overline{\psi}^{\,\mu}(\rho^i\, \partial_i \\ &+ iq\rho^\alpha A_\alpha)\psi_\mu + \frac{1}{2} F^{ij}\, F_{ij}] + \lambda_{\overline{\psi}} p^\mu_{\overline{\psi}} + \lambda_\psi (p^\mu_\psi - \frac{i}{2\pi}\overline{\psi}^\mu \rho^0) + \lambda_1 \pi_0\,, \end{aligned} \tag{35}$$

where $\lambda_{\overline{\psi}}$, λ_ψ and λ_1 are Lagrange multipliers to be determined. From the consistency conditions, the time derivative of the primary constraints should be zero, that is

$$\dot{H'}_{\overline{\psi}} = \{H'_{\overline{\psi}}\,, H_T\} = \frac{1}{2\pi}(i\rho^i \partial_i - q\rho^\alpha\, A_\alpha)\psi_\mu + \frac{i}{2\pi}\rho^0\, \lambda_\psi \approx 0\,, \tag{36}$$

$$\dot{H'}_\psi = \{H'_\psi\,, H_T\} = -\frac{1}{2\pi}\overline{\psi}^{\,\mu}(i\overleftarrow{\partial_i}\rho^i + q\rho^\alpha\, A_\alpha) - \frac{i}{2\pi}\lambda_{\overline{\psi}}\rho^0 \approx 0\,, \tag{37}$$

$$\dot{H'}_1 = \{H'_1, H_T\} = \partial_i \pi^i - \frac{1}{2\pi}\, q\overline{\psi}^{\,\mu}\rho^0 \psi_\mu \approx 0\,. \tag{38}$$

Relations (36) and (37) fix the multipliers λ_ψ and $\lambda_{\overline{\psi}}$ respectively as

$$\lambda_\psi = -(\rho^0\, \rho^i\, \partial_i + iq\, \rho^0\, \rho^\alpha\, A_\alpha)\, \psi_\mu\,, \tag{39}$$

$$\lambda_{\overline{\psi}} = -\overline{\psi}^{\,\mu}(\overleftarrow{\partial_i}\, \rho^i\, \rho^0 - iq\, \rho^\alpha\, \rho^0\, A_\alpha)\,. \tag{40}$$

Eq. (38) lead to the secondary constraints

$$H_1'' = \partial_i \pi^i - \frac{1}{2\pi} q\overline{\psi}^{\,\mu} \rho^0 \psi_\mu \approx 0\,. \tag{41}$$

There are no tertiary constraints, since

$$\dot{H''}_1 = \{H_1'', H_T\} = 0\,. \tag{42}$$

By taking suitable linear combinations of constraints, one has to find the first-class, that is

$$\Phi_1 = H_1' = \pi_0\,, \tag{43}$$

whereas the constraints

$$\Phi_2 = H'_{\overline{\psi}} = p^\mu_{\overline{\psi}}\,, \tag{44}$$

$$\Phi_3 = H'_\psi = p^\mu_\psi - \frac{i}{2\pi}\,\overline{\psi}^{\,\mu} \rho^0\,, \tag{45}$$

$$\Phi_4 = H_1'' = \partial_i \pi^i - \frac{1}{2\pi} q\overline{\psi}^{\,\mu} \rho^0 \psi_\mu\,, \tag{46}$$

are second-class.
The equations of motion read as

$$\dot{X}^\mu = \{X^\mu, H_T\} = -\pi\, p^\mu\,, \tag{47}$$

$$\dot{\overline{\psi}}^{\,\mu} = \{\overline{\psi}^{\,\mu}, H_T\} = \lambda_{\overline{\psi}}\,, \tag{48}$$

$$\dot{\psi}^{\,\mu} = \{\psi_\mu, H_T\} = \lambda_\psi\,, \tag{49}$$

$$\dot{A}^i = \{A^i, H_T\} = -(\pi\, \pi^i - \partial_i A_0)\,, \tag{50}$$

$$\dot{A}^0 = \{A^0, H_T\} = \lambda_1\,, \tag{51}$$

$$\dot{p}_\mu = \{p_\mu, H_T\} = \frac{1}{\pi}\,\partial^i \partial_i X^\mu\,, \tag{52}$$

$$\dot{p^\mu_{\overline{\psi}}} = \{p^\mu_{\overline{\psi}}, H_T\} = \frac{1}{2\pi}\left[(i\rho^i\,\partial_i - q\rho^\alpha\, A_\alpha)\psi_\mu + i\lambda_\psi\,\rho^0\right], \tag{53}$$

$$\dot{p}^{\mu}_{\psi} = \{p^{\mu}_{\psi}\,, H_T\} = -\frac{i}{2\pi}\,\overline{\psi}^{\,\mu}(\overleftarrow{\partial_i}\,\rho^i + iq\,\rho^{\alpha}\,A_{\alpha})\,, \tag{54}$$

$$\dot{\pi}^i = \{\pi^i, H_T\} = \frac{1}{2\pi}\,(2\partial^l F_{il} - q\,\overline{\psi}^{\,\mu}\,\rho^i\,\psi_{\mu})\,, \tag{55}$$

$$\dot{\pi}^0 = \{\pi^0, H_T\} = \partial_i \pi^i\, - \frac{1}{2\pi}\,q\,\overline{\psi}^{\,\mu}\,\rho^0\,\psi_{\mu}\,. \tag{56}$$

Substituting from Eq. (40) into Eq. (48), we get

$$i\overline{\psi}^{\,\mu}\rho^{\alpha}(\overleftarrow{\partial_{\alpha}} - iqA_{\alpha}) = 0\,, \tag{57}$$

and from Eq. (39) into Eqs. (49) and (53), we have

$$i(\partial_{\alpha} + iqA_{\alpha})\rho^{\alpha}\,\psi_{\mu} = 0\,, \tag{58}$$

$$\dot{p}^{\mu}_{\overline{\psi}} = 0\,. \tag{59}$$

We will contact oureselves with a partial gauge fixing by introducing gauge constraints for the first class primary constraints only, just to fix the multiplier λ_1 in Eq. (35). Since π^0 is vanishing weakly, a gauge choice near at hand would be

$$\Phi'_1 = A_0 = 0\,. \tag{60}$$

But for this forbids dynamics at all, since the requirement $\dot{A}_0 = 0$ implies $\lambda_1 = 0$.
In the following section the same system will be discussed using Hamilton-Jacobi approach.

4.2 Hamilton-Jacobi formulation of superstring

The set of Hamilton-Jacobi Partial Differential Equations (HJPDE) (7) read as

$$H'_0 = p_0 + H_0 = 0\,, \tag{61}$$

$$H'_{\overline{\psi}} = p^{\mu}_{\overline{\psi}} + H_{\overline{\psi}} = p^{\mu}_{\overline{\psi}} = 0\,, \tag{62}$$

$$H'_{\psi} = p^{\mu}_{\psi} + H_{\psi} = p^{\mu}_{\psi} - \frac{i}{2\pi}\,\overline{\psi}^{\,\mu}\rho^0 = 0\,, \tag{63}$$

$$H_1' = \pi_0 + H_1 = \pi_0 = 0\,. \tag{64}$$

The equations of motion are obtained as total differential equations follows:

$$\begin{aligned} dX^\mu &= \frac{\partial H_0'}{\partial p_\mu}\,dt + \frac{\partial H_{\overline{\psi}}'}{\partial p_\mu}\,d\overline{\psi}^{\,\mu} + \frac{\partial H_\psi'}{\partial p_\mu}\,d\psi_\mu + \frac{\partial H_1'}{\partial p_\mu}\,dA^0 \\ &= -\pi\, p^\mu\, dt\,, \end{aligned} \tag{65}$$

$$\begin{aligned} dA^i &= \frac{\partial H_0'}{\partial \pi_i}\,dt + \frac{\partial H_{\overline{\psi}}'}{\partial \pi_i}\,d\overline{\psi}^{\,\mu} + \frac{\partial H_\psi'}{\partial \pi_i}\,d\psi_\mu + \frac{\partial H_1'}{\partial \pi_i}\,dA^0 \\ &= -(\pi\,\pi^i - \partial_i A_0)\,dt\,, \end{aligned} \tag{66}$$

$$\begin{aligned} dp_\mu &= -\frac{\partial H_0'}{\partial X_\mu}\,dt - \frac{\partial H_{\overline{\psi}}'}{\partial X_\mu}\,d\overline{\psi}^{\,\mu} - \frac{\partial H_\psi'}{\partial X_\mu}\,d\psi_\mu - \frac{\partial H_1'}{\partial X_\mu}\,dA^0 \\ &= \frac{1}{\pi}\,\partial^i\partial_i X^\mu\,dt\,, \end{aligned} \tag{67}$$

$$\begin{aligned} dp^\mu_{\overline{\psi}} &= -\frac{\partial H_0'}{\partial \overline{\psi}^{\,\mu}}\,dt - \frac{\partial H_{\overline{\psi}}'}{\partial \overline{\psi}^{\,\mu}}\,d\overline{\psi}^{\,\mu} - \frac{\partial H_\psi'}{\partial \overline{\psi}^{\,\mu}}\,d\psi_\mu - \frac{\partial H_1'}{\partial \overline{\psi}^{\,\mu}}\,dA^0 \\ &= \frac{1}{2\pi}\,(i\rho^i\,\partial_i - q\rho^\alpha\,A_\alpha)\psi_\mu\,dt + \frac{i}{2\pi}\,\rho^0 d\psi_\mu\,, \end{aligned} \tag{68}$$

$$\begin{aligned} dp^\mu_\psi &= -\frac{\partial H_0'}{\partial \psi_\mu}\,dt - \frac{\partial H_{\overline{\psi}}'}{\partial \psi_\mu}\,d\overline{\psi}^{\,\mu} - \frac{\partial H_\psi'}{\partial \psi_\mu}\,d\psi_\mu - \frac{\partial H_1'}{\partial \psi_\mu}\,dA^0 \\ &= -\frac{1}{2\pi}(i\,\partial_i\,\overline{\psi}^{\,\mu}\,\rho^i + q\,\overline{\psi}^{\,\mu}\,\rho^\alpha\,A_\alpha)\,dt\,, \end{aligned} \tag{69}$$

$$\begin{aligned} d\pi^i &= -\frac{\partial H_0'}{\partial A_i}\,dt - \frac{\partial H_{\overline{\psi}}'}{\partial A_i}\,d\overline{\psi}^{\,\mu} - \frac{\partial H_\psi'}{\partial A_i}\,d\psi_\mu - \frac{\partial H_1'}{\partial A_i}\,dA^0 \\ &= \frac{1}{2\pi}\,(2\partial^l F_{il} - q\,\overline{\psi}^{\,\mu}\,\rho^i\,\psi_\mu)\,dt\,, \end{aligned} \tag{70}$$

$$d\pi^0 = -\frac{\partial H'_0}{\partial A_0}\,dt - \frac{\partial H'_{\overline{\psi}}}{\partial A_0}\,d\overline{\psi}^{\,\mu} - \frac{\partial H'_{\psi}}{\partial A_0}\,d\psi_\mu - \frac{\partial H'_1}{\partial A_0}\,dA^0$$
$$= (\partial_i \pi^i - \frac{1}{2\pi}\,q\,\overline{\psi}^{\,\mu}\,\rho^0\,\psi_\mu)dt\,. \tag{71}$$

The integrability conditions imply that the variation of the constraints $H'_{\overline{\psi}}$, H'_{ψ} and H'_1 should be identically zero; that is

$$dH'_{\overline{\psi}} = dp^{\mu}_{\overline{\psi}} = 0\,, \tag{72}$$

$$dH'_{\psi} = dp^{\mu}_{\psi} - \frac{i}{2\pi}\,d\overline{\psi}^{\,\mu}\rho^0 = 0\,, \tag{73}$$

$$dH'_1 = d\pi_0 = 0\,. \tag{74}$$

The vanishing of total differential of H'_1 leads to a new constraints

$$H''_1 = \partial_i \pi^i - \frac{1}{2\pi}\,q\overline{\psi}^{\,\mu}\rho^0\psi_\mu\,. \tag{75}$$

When we taking a gain the total differential of H''_1, we notice that it vanishes identically,

$$dH''_1 = 0\,. \tag{76}$$

From Eqs. (65) and (66), respectively we obtain

$$\dot{X}^\mu = -\pi\,p^\mu\,, \tag{77}$$

and

$$\dot{A}^i = -(\pi\,\pi^i - \partial_i A_0)\,. \tag{78}$$

Substituting from Eqs. (68) and (69) into Eqs. (72) and (73) respectively, we get

$$i(\partial_\alpha + iqA_\alpha)\rho^\alpha\,\psi_\mu = 0\,, \tag{79}$$

$$i\overline{\psi}^{\,\mu}\rho^\alpha(\overleftarrow{\partial}_\alpha - iqA_\alpha) = 0\,. \tag{80}$$

Also from Eqs. (67) and (69 - 71), we get the following equations of motion:

$$\dot{p}_\mu = \frac{1}{\pi}\,\partial^i\partial_i X^\mu\,, \tag{81}$$

$$\dot{p}^{\mu}_{\psi} = -\frac{i}{2\pi}\,\overline{\psi}^{\,\mu}(\overleftarrow{\partial_i}\,\rho^i + iq\,\rho^{\alpha}\,A_{\alpha})\,, \tag{82}$$

$$\dot{\pi}^i = \frac{1}{2\pi}\,(2\partial^l F_{il} - q\,\overline{\psi}^{\,\mu}\,\rho^i\,\psi_{\mu})\,, \tag{83}$$

$$\dot{\pi}^0 = \partial_i \pi^i \; - \frac{1}{2\pi}\,q\,\overline{\psi}^{\,\mu}\,\rho^0\,\psi_{\mu}\,. \tag{84}$$

Substituting from Eq.(79) into Eq.(68), we have

$$\dot{p}^{\mu}_{\overline{\psi}} = 0\,. \tag{85}$$

As a comparison between the above two methods, we get that the Hamilton-Jacobi method and Dirac's method give the same equations of motion.

5 Path Integral Quantization of The Relativistic Local Free Field Theory

As an example of a singular system described by a first-order action, namely a system whose Lagrange function is linear in the velocities. However, the associated constraints are all second-class. Let us consider the relativistic local free field theory of spin $\frac{1}{2}$ in a Minkowski spacetime of dimension D. As usual, spacetime coordinates are denoted as $x^{\mu}, y^{\mu}(\mu = 0, 1, \ldots, D-1)$ and space components are labelled by $i, j = 1, 2, \ldots, D-1$. The Minkowski matrix $\eta^{\mu\nu}$ is chosen with a signature with mostly minus signs, and we also set $\hbar = c = 1$. The system is described by the first-order action

$$S[\psi] = \int d^D x\, l(\psi, \partial_{\mu}\psi). \tag{86}$$

with the local lagrangian density function

$$l(\psi, \partial_{\mu}\psi) = i\frac{\lambda+1}{2}\,\overline{\psi}\gamma^{\mu}\partial_{\mu}\psi + i\frac{\lambda-1}{2}\,\partial_{\mu}\overline{\psi}\gamma^{\mu}\psi - m\overline{\psi}\psi\,. \tag{87}$$

Here λ is a parameter, the matrices γ^{μ} define the Dirac algebra in D-dimensional Minkowski spacetime

$$\{\gamma^{\mu}, \gamma^{\nu}\} = 2\,\eta^{\mu\nu}, \quad \gamma^{\mu\dagger} = \gamma^0\gamma^{\mu}\gamma^0\,, \tag{88}$$

and $\psi_\alpha(x)(\alpha = 1, 2, \ldots, 2^{[D/2]})$ are Grassmann even degrees of freedom defining a Dirac spinor, with

$$\overline{\psi}(x) = \psi^\dagger(x)\,\gamma^0\,. \tag{89}$$

For simplicity, the fields $\psi(x)$ are assumed to fall off sufficiently rapidly at infinity for all practical purposes.
The Lagrangian (87) is singular, since the rank of the Hess matrix (1) is zero.
Let us first discuss the system using Hamilton-Jacobi approach. In this approach the canonical momenta (2) and (3) take the forms

$$p = \frac{\partial L}{\partial \partial_0 \psi} = i\frac{\lambda+1}{2}\,\overline{\psi}\gamma^0 = -H\,, \tag{90}$$

and

$$\overline{p} = \frac{\partial L}{\partial \partial_0 \overline{\psi}} = i\frac{\lambda-1}{2}\,\gamma^0\psi = -\overline{H}\,. \tag{91}$$

where we must call attention to the necessity of being careful with the spinor indexes. Considering, as usual ψ as a column vector and $\overline{\psi}$ as a row vector implies that p will be a row vector while $\overline{p}$ will be a column vector.
The usual Hamiltonian H_0 is given as

$$H_0 = -L + \partial_0\psi\, p_\mu + \partial_0\overline{\psi}\, p_{\overline{\mu}}\Big|_{p_\mu = -H_\mu,\, p_{\overline{\mu}} = -H_{\overline{\mu}}}\,, \tag{92}$$

or,

$$H_0 = -i\frac{\lambda+1}{2}\,\overline{\psi}\gamma^a\partial_a\psi - i\frac{\lambda-1}{2}\,\partial_a\overline{\psi}\gamma^a\psi + m\overline{\psi}\psi\,, \qquad a = 1,2,3\,. \tag{93}$$

The set of Hamilton-Jacobi partial differential equation (HJPDE) are

$$H_0' = p_0 + H_0 = p_0 - i\frac{\lambda+1}{2}\,\overline{\psi}\gamma^a\partial_a\psi - i\frac{\lambda-1}{2}\,\partial_a\overline{\psi}\gamma^a\psi + m\overline{\psi}\psi\,, \tag{94}$$

$$H' = p + H = p - i\frac{\lambda+1}{2}\,\overline{\psi}\gamma^0 = 0\,, \tag{95}$$

$$\overline{H'} = \overline{p} + \overline{H} = \overline{p} - i\frac{\lambda-1}{2}\,\gamma^0\psi = 0\,. \tag{96}$$

Therefor, the total differential equations for the characteristic (14 - 16) are:

$$d\psi = d\psi\,, \tag{97}$$

$$d\overline{\psi} = d\overline{\psi}\,, \tag{98}$$

$$dp = \left(i\frac{\lambda-1}{2}\,\partial_a\overline{\psi}\gamma^a - m\overline{\psi}\right)d\tau + i\frac{\lambda-1}{2}\,\gamma^0 d\overline{\psi}\,, \tag{99}$$

$$d\overline{p} = \left(i\frac{\lambda+1}{2}\,\partial_a\psi\gamma^a - m\psi\right)d\tau + i\frac{\lambda+1}{2}\,\gamma^0 d\psi\,. \tag{100}$$

To check wether the set of equations (97 - 100) is integrable or not, we have to consider the total variation of the constraints. In fact

$$dH' = dp - i\frac{\lambda+1}{2}\,\gamma^0 d\overline{\psi} = 0\,, \tag{101}$$

$$d\overline{H'} = d\overline{p} - i\frac{\lambda-1}{2}\,\gamma^0 d\psi = 0\,. \tag{102}$$

The constraints (95) and (96), lead us to obtain

$$d\overline{\psi} = i(i\partial_a\overline{\psi}\gamma^a + m\overline{\psi})\gamma^0 dt\,, \tag{103}$$

and

$$d\psi = i\gamma^0(i\gamma^a\partial_a\psi - m\psi)dt\,. \tag{104}$$

Then, we conclude that the set of equations (97 - 100) is integrable.

Making use of Eq. (17) and Eqs. (94 - 96), we can write the canonical action integral as

$$Z = \int d^4x\left(i\frac{\lambda+1}{2}\,\overline{\psi}\gamma^\mu\partial_\mu\psi + i\frac{\lambda-1}{2}\,\partial_\mu\overline{\psi}\gamma^\mu\psi - m\overline{\psi}\psi\right). \tag{105}$$

Now the S-matrix element is given by

$$\left\langle \psi,\overline{\psi},\iota;\psi',\overline{\psi}',\iota\right\rangle = \int d\psi\, d\overline{\psi}$$
$$exp\left[i\left\{\int d^4x\left(i\frac{\lambda+1}{2}\,\overline{\psi}\gamma^\mu\partial_\mu\psi + i\frac{\lambda-1}{2}\,\partial_\mu\overline{\psi}\gamma^\mu\psi - m\overline{\psi}\psi\right)\right\}\right]. \tag{106}$$

Now we will apply the Senjanovic method to the previous example. The total Hamiltonian is given as

$$H_T = H_0 + \nu H' + \overline{\nu}\overline{H'}\,, \tag{107}$$

or

$$H_T = -i\frac{\lambda+1}{2}\,\overline{\psi}\gamma^a\partial_a\psi - i\frac{\lambda-1}{2}\,\partial_a\overline{\psi}\gamma^a\psi + m\overline{\psi}\psi \\ + \nu(p - i\frac{\lambda+1}{2}\,\overline{\psi}\gamma^0) + \overline{\nu}(\overline{p} - i\frac{\lambda-1}{2}\,\gamma^0\psi)\,, \tag{108}$$

where ν and $\overline{\nu}$ are Lagrange multipliers to be determined. From the consistency conditions, the time derivative of the primary constraints should be zero, that is

$$\dot{H'} = \{H', H_T\} = -i\partial_a\overline{\psi}\,\gamma^a - m\overline{\psi} - i\,\overline{\nu}\,\gamma^0 \approx 0\,, \tag{109}$$

$$\dot{\overline{H}'} = \{\overline{H}', H_T\} = i\,\gamma^a\,\partial_a\psi - m\,\psi + i\,\gamma^0\nu \approx 0\,. \tag{110}$$

Eqs. (109) and (110) fix the multipliers $\overline{\nu}$ and ν, respectively as

$$\overline{\nu} = -\overline{\psi}(\overleftarrow{\partial_a}\gamma^a - im)\gamma^0\,, \tag{111}$$

and

$$\nu = -\gamma^0(\gamma^a\,\partial_a + im)\,\psi\,. \tag{112}$$

There are no secondary constraints. By taking suitable linear combinations of constraints, one has to find the maximal number of second class only, there are

$$\Phi_1 = H' = p - i\frac{\lambda+1}{2}\,\overline{\psi}\gamma^0\,, \tag{113}$$

and

$$\Phi_2 = \overline{H}' = \overline{p} - i\frac{\lambda-1}{2}\,\gamma^0\psi\,. \tag{114}$$

The total Hamiltonian is vanishing weakly. It can completely be written in terms of second-class constraints as

$$H_T = -i\frac{\lambda+1}{2}\,\overline{\psi}\gamma^a\partial_a\psi - i\frac{\lambda-1}{2}\,\partial_a\overline{\psi}\gamma^a\psi + m\overline{\psi}\psi + \nu\,\Phi_1 + \overline{\nu}\Phi_2\,. \tag{115}$$

The equations of motion are read as

$$\dot{\psi} = \{\psi, H_T\} = \nu\,, \tag{116}$$

$$\dot{\overline{\psi}} = \{\overline{\psi}, H_T\} = \overline{\nu}\,, \tag{117}$$

$$\dot{p} = \{p, H_T\} = -i\partial_a \overline{\psi}\gamma^a - m\overline{\psi} + i\overline{\nu}\,\frac{\lambda-1}{2}\,\gamma^0\,, \tag{118}$$

and

$$\dot{\overline{p}} = \{\overline{p}, H_T\} = i\gamma^a\partial_a\psi - m\psi + i\nu\,\frac{\lambda+1}{2}\,\gamma^0\,. \tag{119}$$

To obtain the path integral quantization, taking into our consideration that we have two constraints (primary constraint), which are second-class constraints, then we make use the Senjanovic method Eq. (22) one obtains

$$\begin{aligned}\langle Out|S|In\rangle = \int exp\Big[i\int_{-\infty}^{+\infty}\Big(i\frac{\lambda+1}{2}\overline{\psi}\gamma^\mu\partial_\mu\psi + i\frac{\lambda-1}{2}\,\partial_\mu\overline{\psi}\gamma^\mu\psi - m\overline{\psi}\psi\Big)\Big] \\ dt\,D\psi\,DpD\overline{\psi}\;D\overline{p}\;\det(\gamma^0 I) \\ \times\;\delta(p - i\frac{\lambda+1}{2}\,\overline{\psi}\gamma^0)\,\delta(\overline{p} - i\frac{\lambda-1}{2}\gamma^0\psi)\,.\end{aligned} \tag{120}$$

After integrating over p and $\overline{p}$ one can arrive at the result which has seen in Eq. (106).

6 Hamilton-Jacobi quantization of the scalar field coupled to two fLavours of fermions through yukawa couplings

We consider one loop order the self-energy for the scalar field φ with a mass m, coupled to two flavours of fermions with masses m_1 and m_2, coupled through Yukawa couplings described by the lagrangian

$$\begin{aligned}L = \frac{1}{2}(\partial_\mu\varphi)^2 - \frac{1}{2}m^2\varphi^2 - \frac{1}{6}\lambda\varphi^3 + \sum_i \overline{\psi}_{(i)}(i\gamma^\mu\partial_\mu - m_i)\psi_{(i)} \\ - g\varphi(\overline{\psi}_{(1)}\psi_{(2)} + \overline{\psi}_{(2)}\psi_{(1)}), \qquad \mu = 0,1,2,3\,,\end{aligned} \tag{121}$$

where λ is parameter and g constant, φ, $\psi_{(i)}$, and $\overline{\psi}_{(i)}$ are odd ones. We are adopting the Minkowski metric $\eta_{\mu\nu} = diag(+1,-1,-1,-1)$.

The Lagrangian function (121) is singular, since the rank of the Hess matrix (1) is one. The generalized momenta (2, 3) are

$$p_\varphi = \frac{\partial L}{\partial \dot{\varphi}} = \partial^0 \varphi\,, \tag{122}$$

$$p_{(i)} = \frac{\partial L}{\partial \dot{\psi}_{(i)}} = i\overline{\psi}_{(i)}\gamma^0 = -H_{(i)}, \qquad i = 1,2\,, \tag{123}$$

$$\overline{p}_{(i)} = \frac{\partial L}{\partial \dot{\overline{\psi}}_{(i)}} = 0 = -\overline{H}_{(i)}\,. \tag{124}$$

Where we must call attention to the necessity of being careful with the spinor indexes. Considering, as usual $\psi_{(i)}$ as a column vector and $\overline{\psi}_{(i)}$ as a row vector implies that $p_{(i)}$ will be a row vector while $\overline{p}_{(i)}$ will be a column vector.

Since the rank of the Hess matrix is one, one may solve (122) for $\partial^0\varphi$ as

$$\partial^0 \varphi = p_\varphi \equiv \omega\,. \tag{125}$$

The usual Hamiltonian H_0 is given as

$$H_0 = -L + \omega p_\varphi + \partial_0\psi_{(i)}\, p_{(i)}\Big|_{p_{(i)}=-H_{(i)}} + \partial_0\overline{\psi}_{(i)}\,\overline{p}_{(i)}\Big|_{\overline{p}_{(i)}=-\overline{H}_{(i)}}\,, \tag{126}$$

or

$$\begin{aligned} H_0 = \frac{1}{2}({p^2}_\varphi - \partial_a\varphi\partial^a\varphi) + \frac{1}{2}m^2\varphi^2 + \frac{1}{6}\lambda\varphi^3 - \overline{\psi}_{(i)}(i\gamma^a\partial_a - m_i)\psi_{(i)} \\ + g\varphi(\overline{\psi}_{(1)}\psi_{(2)} + \overline{\psi}_{(2)}\psi_{(1)})\,, \qquad a = 1,2,3\,. \end{aligned} \tag{127}$$

The set of Hamilton-Jacobi Partial Differential Equations (7) and (8) read as

$$\begin{aligned} H_0' &= p_0 + H_0 \\ &= p_0 + \frac{1}{2}({p^2}_\varphi - \partial_a\varphi\partial^a\varphi) + \frac{1}{2}m^2\varphi^2 + \frac{1}{6}\lambda\varphi^3 - \overline{\psi}_{(i)}(i\gamma^a\partial_a - m_i)\psi_{(i)} \\ &\quad + g\varphi(\overline{\psi}_{(1)}\psi_{(2)} + \overline{\psi}_{(2)}\psi_{(1)})\,, \end{aligned} \tag{128}$$

$$H'_{(i)} = p_{(i)} + H_{(i)} = p_{(i)} - i\,\overline{\psi}_{(i)}\,\gamma^0 = 0\,, \tag{129}$$

$$\overline{H}'_{(i)} = \overline{p}_{(i)} + \overline{H}_{(i)} = \overline{p}_{(i)} = 0\,. \tag{130}$$

Therefor, the total differential equations for the characteristic (14 - 16) are:

$$d\varphi = p_\varphi d\tau\,, \tag{131}$$

$$d\psi_{(i)} = d\psi_{(i)}\,, \tag{132}$$

$$d\overline{\psi}_{(i)} = d\overline{\psi}_{(i)}\,, \tag{133}$$

$$dp_\varphi = \left[m^2\varphi + \frac{1}{2}\lambda\varphi^2 + g(\overline{\psi}_{(1)}\psi_{(2)} + \overline{\psi}_{(2)}\psi_{(1)})\right]d\tau\,, \tag{134}$$

$$dp_{(1)} = \left[\overline{\psi}_{(1)}(i\overleftarrow{\partial}_a\gamma^a + m_1) + g\,\varphi\,\overline{\psi}_{(2)}\right]d\tau\,, \tag{135}$$

$$dp_{(2)} = \left[\overline{\psi}_{(2)}(i\overleftarrow{\partial}_a\gamma^a + m_2) + g\,\varphi\,\overline{\psi}_{(1)}\right]d\tau\,, \tag{136}$$

$$d\overline{p}_{(1)} = \left[-(i\gamma^a\partial_a - m_1)\psi_{(1)} + g\varphi\psi_{(2)}\right]d\tau - i\gamma^0 d\psi_{(1)}\,, \tag{137}$$

and

$$d\overline{p}_{(2)} = \left[-(i\gamma^a\partial_a - m_2)\psi_{(2)} + g\varphi\psi_{(1)}\right]d\tau - i\gamma^0 d\psi_{(2)}\,. \tag{138}$$

To check whether the set of equations (131 - 138) is integrable or not, we have to consider the total variations of the constraints. In fact

$$dH'_{(i)} = dp_{(i)} - i\,d\overline{\psi}_{(i)}\,\gamma^0 = 0\,, \tag{139}$$

$$d\overline{H}'_{(i)} = d\overline{p}_{(i)} = 0\,. \tag{140}$$

The constraints (129) and (130), lead us to obtain $d\overline{\psi}_{(i)}$ and $d\psi_{(i)}$ in terms of dt

$$d\overline{\psi}_{(1)}i\gamma^0 = [\overline{\psi}_{(1)}(i\overleftarrow{\partial_a}\gamma^a + m_1) + g\varphi\,\overline{\psi}_{(2)}]dt\,, \tag{141}$$

$$d\overline{\psi}_{(2)}i\gamma^0 = [\overline{\psi}_{(2)}(i\overleftarrow{\partial_a}\gamma^a + m_2) + g\varphi\,\overline{\psi}_{(1)}]dt\,, \tag{142}$$

$$i\gamma^0 d\psi_{(1)} = [-(i\gamma^a\partial_a - m_1)\psi_{(1)} + g\,\varphi\,\psi_{(2)}]d\,, \tag{143}$$

and

$$i\gamma^0 d\psi_{(2)} = [-(i\gamma^a\partial_a - m_2)\psi_{(2)} + g\,\varphi\,\psi_{(1)}]dt\,. \tag{144}$$

We obtain that the set of equations (131 - 138) is integrable. Making use of (17), and (128 - 130), we can write the canonical action integral as

$$Z = \int d^4x[\frac{1}{2}(p^2{}_\varphi + \partial_a\varphi\partial^a\varphi) - \frac{1}{2}m^2\varphi^2 - \frac{1}{6}\lambda\varphi^3 + \overline{\psi}_{(i)}(i\gamma^\mu\partial_\mu - m_i)\psi_{(i)} - g\varphi(\overline{\psi}_{(1)}\psi_{(2)} + \overline{\psi}_{(2)}\psi_{(1)})]\,, \tag{145}$$

Now the path integral representation (24) is given by

$$\langle out|S|In\rangle = \int \prod_i^2 d\varphi\, dp_\varphi\, d\psi_{(i)}\, d\overline{\psi}_{(i)} \; exp\left\{i\left[\int d^4x\frac{1}{2}(p^2{}_\varphi + \partial_a\varphi\partial^a\varphi) - \frac{1}{2}m^2\varphi^2 - \frac{1}{6}\lambda\varphi^3 + \overline{\psi}_{(i)}(i\gamma^\mu\partial_\mu - m_i)\psi_{(i)} - g\varphi(\overline{\psi}_{(1)}\psi_{(2)} + \overline{\psi}_{(2)}\psi_{(1)})\right]\right\}. \tag{146}$$

7 Conclusion

In this paper, we have investigated three different constrained systems. Two of them are studied by using Dirac's Hamiltonian formalism and Hamilton-Jacobi approach. The third one quantized by Hamilton-Jacobi quantization.

We have treated constrained system of the Lagrangian describing superstring and have obtained the equations of motion of this system by Dirac's and Hamilton-Jacobi method. In the Dirac method the total Hamiltonian composed by adding the constraints multiplied by Lagrange multipliers to

the canonical Hamiltonian. In order to drive the equations of motion, one needs to redefine these unknown multipliers in an arbitrary way. However, in the Hamilton-Jacobi formalism, there is no need to introduce Lagrange multipliers to the canonical Hamiltonian. Both the consistency conditions and integrability conditions lead to the same constraints. In the Hamilton-Jacobi formulation, the equations of motion are obtained directly by using HJPDES as total differential equations.

Path integral quantization of the relativistic local free field theory is obtained by using the Senjanovic method and the Hamilton-Jacobi path integral formulation. Both methods give the same results. However, in the Hamilton-Jacobi path integral formulation, since the integrability conditions dH' and $d\overline{H}'$ are satisfied, so this system is integrable, and hence the path integral is obtained directly as an integration over the canonical phase-space coordinates $(\psi, \overline{\psi})$. In the usual formulation, one has to integrate over the extended phase-space $(p, \psi, \overline{p}, \overline{\psi})$ and one can get rid of the redundant variables $(p, \overline{p})$ by using delta function $\delta(p - i\frac{\lambda+1}{2}\overline{\psi}\gamma^0)$ and $\delta(\overline{p} - i\frac{\lambda-1}{2}\gamma^0\psi)$. Furthermore, the scalar field coupled to two flavours of fermions through Yukawa couplings are quantized as a constrained system by using Hamilton-Jacobi quantization. That is no need to introduce Lagrange multipliers to the canonical Hamiltonian, then the Hamilton-Jacobi is simpler and more economical.

As a conclusion, the Hamilton-Jacobi approach is always in exact agreement with Dirac's method. Both the consistency conditions and integrability conditions lead to the same constraints. The singular system with second-class constraints is quantized by Hamilton-Jacobi quantization successfully. The Hamilton-Jacobi path integral quantization is simpler and more economical. In Hamilton-Jacobi treatment, there is no need to distinguish between first-class and second-class constraints, and there is no need to introduce Lagrange multipliers; all that is needed is the set of Hamilton-Jacobi partial differential equations and the equations of motion. If the system is integrable then one can construct the canonical phase space. In hamilton-Jacobi quantization, the gauge fixing is not necessary to obtain the path integral formulation for field theories if the canonical formulation is used. Since this system is integrable, the path integral is obtained as an integration over the canonical phase-space coordinates.

References

[1] P. A. M. Dirac, Can. J. Math. **2**, 129 (1950).

[2] P. A. M. Dirac, "*Lectures on Quantum Mechanics*", Belfer Graduate school of science, Yehiva university (A cademic press, New yourk) (1964).

[3] D. M. Gitman and I.V. Tyutin, "*Quantization of Fields with constraints*", Springs verlag, Berlin (1990).

[4] M. Henneaux and C. Teitelboim, "*Quantization of Gauge Systems*", Princeton University Press, Princeton, New Jersey (1992).

[5] Y. Güler, Nuovo Cimento **B107**, 1389 (1992).

[6] Y. Güler, Nuovo Cimento **B107**, 1143 (1992).

[7] Y. Güler, Nuovo Cimento **B100**, 251, 267 (1987); J. Math. Phys. **30**, 785 (1989).

[8] N. I. Farahat and Y. Güler, Nuovo Cimento **B111**, 513 (1996).

[9] S. I. Muslih and Y. Güler, Nuovo Cimento **B113**, 277 (1998).

[10] D. Baleanu and Y. Guler, Nuovo Cim. B **115**, 25 (2000) [hep-th/9901097].

[11] W. I. Eshraim and N. I. Farahat, Hadronic J., no. 29, 553 (2006).

[12] W. I. Eshraim and N. I. Farahat, Electron. J. Theor. Phys. **5**, no. 17, 65 (2008).

[13] W. I. Eshraim and N. I. Farahat, Rom. J. Phys. **53**, 437 (2008).

[14] R. M. Santilli, "*FounationsofTheoreticalMechanics*", Vol. II, Springer-Verlag, Berlin (1983).

[15] L.D. Faddeev, Teoret. Mat. Fiz. **1**, 3 (1969) [Theor. Math. Phys. **1**, 1 (1970)].

[16] L.D. Faddeev and V. M. Popov, phys. Lett. **B24**, 29 (1967).

[17] P. Senjanovic, Ann. Phys (NY) **100**, 227 (1976).

[18] E. S. Fradkin and G. A Vilkovisky, Phys. Rev. **D8**,4241 (1973).

[19] D. Baleanu and Y. Güler, Int. J. Theor. Phys. **41**, 861 (2002).

[20] S. I. Muslih, N. I. Farahat and M. R. Heles, Nuovo Cim. B **119**, 531 (2004).

[21] W. I. Eshraim and N. I. Farahat, Electron. J. Theor. Phys. **6**, no. 22, 189 (2009).

[22] W. I. Eshraim, Islamic University Journal **18**, 42 (2010) [arXiv:1301.2478 [physics.gen-ph]].

[23] W. I. Eshraim and N. I. Farahat, Electron. J. Theor. Phys. **4**, no. 14, 61 (2007).

[24] S. I. Muslih, Nuovo Cim. B **118**, 505 (2003).

[25] S. I. Muslih, Mod. Phys. Lett. A **19**, 151 (2004).

[26] S. I. Muslih and Y. Güler, Nuovo Cimento **B112**, 531 (1997).

ALGEBRAS GROUPS AND GEOMETRIES 35 389 - 394 (2018)
DOI 10.29083/AGG.35.04.2018

ON RIEMANN CONJECTURE

Jiang Yu
Guangzeng Group, fourth floor, number 10,
Guangming East Road, Zengcheng City,
Post Code: 511316, Guangdong Province, China
jiangyugs@163.com

Received December 18, 2019
Revised April 8, 2020

Abstract

This paper explains the variation of the even and odd number sets in a natural number set, as well as the composite number and prime number sets in an odd number set using the contraction and extension of the coordinate axes. In this study, a new explanation of the Riemann function $\zeta(s)$ is also introduced.

Key words: Natural numbers, even numbers, odd numbers, composite numbers, prime numbers, pattern

Copyright © 2018 by Hadronic Press Inc., Palm Harbor, FL 34682, U.S.A.

1 Introduction

By considering the following, through the contraction and extension of coordinate axes, we demonstrate that linear transformations can produce both even and odd numbers from subsets of a set of composite numbers.

A natural number n means 0, 1, 2, 3, 4, ..., including 0 and the positive integers. The set of natural numbers is represented by N. Natural numbers other than 0 and 1 are successors of the natural number 1, i.e.:

$$n=1+1+1+\ldots$$

This is the basic property of natural numbers. The number n is called a superposition of n natural numbers 1.

A number that can be divided by 2 is called an even number, and the even number set is represented by N_0. Numbers that are not divisible by 2 are called odd numbers, and the odd number set is represented by N_1.

In the odd number set N_1, any natural number indivisible by any factor except for 1 and itself is called a prime number. The set of prime numbers is represented by N_S. Natural numbers that are divisible by other factors are called composite numbers, and the set of composite numbers is represented by N_m.

2 Contraction and extension of coordinate axes

In the following considerations, we agree that n is a natural number, n_n (n_1, n_2, ...) is 0 or an integer, and x and y are arbitrary numbers.

The zeros and intervals of the Cartesian coordinates can be arbitrarily selected. Normally, we select the natural number 0 as the zero point of the coordinate and the natural number 1 as the coordinate interval. This coordinate system is called the "1 × 1" coordinate system and we get:

$$n=n_1. \tag{1}$$

Each interval point of the "1 × 1" coordinate system represents a natural number, and the set of natural numbers is N.

We can also choose the natural number 0 as the zero point of the coordinate and the superposition of n^0 consecutive natural numbers 1 as the coordinate interval. This coordinate system is called the "1 × n^0" coordinate system, and we have

$$n=n^0n_1, \tag{2}$$

$$n^0=1+1+\ldots$$

This process is called a contraction of the coordinate system, the contraction coefficient is expressed by δ^-, and we have:

$$\delta^-=n^0. \tag{3}$$

Each interval point of the "1 × n^0" coordinate system represents a natural number. When $\delta=2$, the set of natural numbers is mapped to N_0 or N_1, which is:

$$n=2n_1, \tag{4}$$

$$n=2n_1-1. \tag{5}$$

Each interval of the "1 × n^0" coordinate system is divided into n^0 equal parts. This process is called an extension of the coordinate system, and the extension coefficient is represented by δ^+; thus, we have:

$$\delta^+=1/n^0. \tag{6}$$

When $\delta^-\delta^+=1$, we get the "1 × 1" coordinate system, and the set of natural numbers is N.

3 Producing even and odd numbers from subsets of a set of composite numbers

The following considerations are based on those given above.

Natural numbers other than 0 and 1 can be represented by the following equation:

$$n=2n_1+3n_2. \quad (7)$$

Given a choice of n_1 and n_2 that satisfies (7), we chose $x=n_1$ as the x-axis of the coordinate system and $y=n_2$ as the y-axis of the coordinate system. As a result, we have the following:

$$n=2x+3y, \quad (8)$$

When $n_2=0$, $n=2n_1$, $N\in 0, 2, 4, 6, \ldots$

When $n_2=1$, $n=2n_1+3$, $N\in 1, 3, 5, 7, 9, \ldots$; the natural number 1 is at $n_1=-1$, $n_2=0$.

Through the following considerations, we obtain the variation pattern of the composite set N_m and the prime set N_s in the odd number set N_1.

For the sake of simplicity, we chose the natural number 3 as the zero of the coordinates ($n=2n_1+3$), and a composite number in the odd number set N_1 can be represented by the following equation:

$$n=(2n_1+3)\times(2n_2+3)=2(2\,n_1\,n_2+3n_1+3n_2+3)+3. \quad (9)$$

Assume

$$n_3=2xy+3x+3y+3. \quad (10)$$

When $n\in N_m$, x and y have one or more than one integer solutions, we have:

$$x=f(n_1), \quad (11)$$

and

$$y=f(n_2). \quad (12)$$

When $n\in N_s$, x or y has no integer solutions, we have:

$$x=f(n_1)+k, \quad (13)$$

or

$$y=f(n_2)+k, \quad (14)$$

where $|k|<1$.

From Equation (9), when $n_2=0$ (when $n_1=0$, the proof is omitted), we have:

$$n=2(3n_1+3)+3. \quad (15)$$

From Equation (15), when $\delta^+=1/3$, we have:

$$n=2n_1+9. \tag{16}$$

We thus have the odd number set N_1. After a simple derivation, we obtain the following three equations:

$$x=n_1, \tag{17}$$

or

$$x=n_1+1/3, \tag{18}$$

or

$$x=n_1+2/3. \tag{19}$$

From Equation (16), when $\delta^+=1/2$, we have the following:

$$n=n_1+9. \tag{20}$$

We thus have the natural number set N. After a simple derivation, we obtain the following two equations:

$$x=n_1, \tag{21}$$

or

$$x=n_1+1/2. \tag{22}$$

Next, we consider Riemann function $\zeta(s)$.

Riemann function $\zeta(s)$ satisfies the following algebraic relations:

$$\zeta(s)=2^s\pi^{s-1}\sin\frac{\pi s}{2}\Gamma(1-s)\zeta(1-s). \tag{23}$$

We already know that the trivial zeros of Riemann function $\zeta(s)$ are at $s=-2n$ and the non-trivial zeros are at $\mathrm{Re}(s)=1/2$.

From Equation (21) and (22), let's translate the x-axis by 1/2, we have the following:

$$x'=x+1/2. \tag{24}$$

From Equation (23) and (24), we have the following:

$$\zeta(s') = 2^{s'}\pi^{s'-1}\sin\frac{\pi s'}{2}\Gamma(1-s')\zeta(1-s'). \quad (25)$$

From Equation (25), we obtain the following conclusions:

The trivial zeros of Riemann function $\zeta(s')$ are at $s' = -(2n+1)$ and the non-trivial zeros are at $\mathrm{Re}(s') = 0$.

Assume

$$0<\mathrm{Re}(s)<1/2,$$

We have the following:

$$2n<|s|<2n+1,$$

Where s is a non-integer.

4 Conclusion

Based on the equations above, it is proved that linear transformations can produce both even and odd numbers from subsets of a set of composite numbers.

References

[1] Gong, Sheng. Concise Calculus (Fourth Edition) [M]. Beijing: Higher Education Press, 2006

[2] Min, Yan. Primary Number Theory [M]. Beijing: Higher Education Press, 2003.

[3] https://www.docin.com/p-1970518235.html

ALGEBRAS GROUPS AND GEOMETRIES 35 395 - 411 (2018)
DOI 10.29083/AGG.35.04.2018

ISONUMBERS AND RGB IMAGE ENCRYPTION

Mamadou I. Wade and Tepper L. Gill
EECS Howard University, Washington, DC 20059
mamadou.wade@howard.edu
tgill@howard.edu

Received May 12, 2020
Revised June 1, 2020

Abstract

In this paper we first discuss isonumber theory, which was developed for applications in physics by R. M. Santilli. We then use isonumbers of the first kind and the Paillier cryptographic system to add an additional security degree of freedom to the image encryption scheme, which we call the Paillier-Senegalese encryption process.

Following standard procedures we first separate a given RGB image into its constituent channel images, use public encryption keys in conjunction with the Paillier-Senegalese encryption function, to encrypt each of the R, G, and B-channel pixel intensity values. The encrypted channel images can be then combined and compressed if necessary before transmission through a possibly unsecured communication channel. The transmitted encrypted image is subsequently recovered by a decryption process which uses the Paillier-Senegalese decryption function in conjunction with the private decryption keys.

We are conducting a number of the performance and security analyses on the recovered and encrypted images in order to study and verify their robustness relative to all desirable security metrics. The complete results of our study will be reported later, but preliminary evidence shows that, the use of isonumbers provide an additional security degree of freedom for the production of encrypted images.

Copyright © 2018 by Hadronic Press Inc., Palm Harbor, FL 34682, U.S.A.

1 Introduction

A number of image encryption schemes have been proposed in the past. Image encryption schemes based on chaos in dynamical systems have been proposed in [3], [15] and [19]. Pareek et al. [19], have developed an encryption scheme which uses a 80-bit encryption key to initialize two chaotic maps. G. Ye et al. [13], have proposed an encryption scheme based on electrocardiography and autoblocking to generate the initial keys, which removes the need for manual assignment. Singh et al. [16] have developed an Elliptic Curve Cryptosystem, which one applies to a group of pixels to obtain a corresponding cipher-image. In another direction, P. P. Dang and P. M. Chau [20], have discussed an encryption scheme which uses the Discrete Wavelet Transform (DWT) for image compression and the block cipher Data Encryption Standard (DES) to produce a secure image. Image encryption using Multi-orders of the Fractional Fourier Transforms has been proposed by R. Tao, X. Meng, and Y. Wang [21]. In this case, the summation of different orders of the inverse discrete Fractional Fourier transform (FRFT) is applied to the interpolated sub-images to create the encrypted image.
This paper explores the application of isonumber theory to red green blue (RGB) image encryption.

Purpose

In this paper we introduce the Paillier-Senegalese image encryption process using the Paillier cryptographic scheme and Santilli's Isonumber Theory of the first kind (see [10]). The isonumber theory replaces the unit "one" of normal arithmetic by a new unit called an "isounit", which provides an additional degree of freedom for the encryption process. We apply our approach to the encryption and decryption of images in the visible range of the electromagnetic spectrum.

The introduction of an isounit may be seen as a shared private encryption and decryption key. We also note that our scheme possesses both public-key and private-key characteristics, so it can be seen as a hybrid public-key and private-key system. The major contribution of this paper is the introduction

of an isounit as a private key and the development of this hybrid public-key and private-key cryptographic system, allowing the improvement of security by increasing the number of decryption keys required for an attacker to gain access to the transmitted images.

Content

The paper is organized as follows: In Section II, we introduce the Santilli's isonumbers theory of the first kind. In Section III, we combine the isonumbers with the Paillier cryptographic scheme to produce Paillier-Senegalese image cryptographic scheme. In Section IV we propose methods that will allow us to analyze the performance and security for our image encryption approach. Section V is devoted to our conclusion.

2 Santilli's Theory of Isonumbers

In this section, we provide a brief introduction to Santilli's Theory of Isonumbers. The origin of isonumbers can be traced at least back to 1978, when Santilli published the second volume of his fundamental work on the "Foundations of Theoretical Mechanics". He was studying the more realistic problem of local physical systems with dissipative forces as opposed to the mathematically beautiful but physically incorrect case of local systems without these forces. As first noted by Santilli, all of the nice mathematics and geometry developed in the twenth century and used in physics to study elementary particles fails. The failure follows because the special theory of relativity does not apply for studies inside the proton (or inside a star), where particles move in dissipative media (and not in a vacuum).

While looking for a way to extend the ideal mathematics, making it more useful for physics, he discovered that all mathematical structures could be preserved by replacing the normal unit by a strictly positive definite unit, which need not be commutative and may depend on any number of physical variables, change with time and have as many derivatives as needed to reproduce experimental reality. This new unit he called an "isotope" (see [5], [7] and [8]). The simplest case is that of the real and complex numbers,

where the unit is the number one. Santilli began his study of this case with his seminal paper on "isonumbers" (see [5] and also [9]).

Our interest is limited to isonumbers. To make the transition easy, we consider the simplest example, which was used by Santilli to represent antiparticles as particles moving backwards in time, providing a rigorous foundation for an idea proposed by Feynman.
The real numbers is a field, which may be represented by a five-tuple $(\mathbb{R}, +, 0, \cdot, 1)$. Where zero is the unit for addition and one is the unit for multiplication. Santilli noticed that mathematicians implicitly use a sense of direction from left to right for $\mathbb{R}$, so that we should write it as a six-tuple $(\mathbb{R}, +, 0, \cdot, 1, \rightarrow)$. It now follows that, in practice, our real number system is not symmetric. Santilli's solution was to propose a new representation of the real numbers $(\hat{\mathbb{R}}, +, 0, *, \hat{1}, \leftarrow)$, where the unit for addition is unchanged, but the new unit for multiplication is now $\hat{1} = -1$. Thus,

$$\hat{a} * \hat{b} = (-a)(-1)(-b) = -ab = \widehat{ab}. \tag{2.1}$$

Santilli called $(\hat{\mathbb{R}}, +, 0, *, \hat{1}, \leftarrow)$ the isotopic dual representation of the real numbers. This is an example of Santilli's Isonumber Theory of the Second Kind, where the new unit, called isounit, is in the field (i.e. $(-1) = \hat{I} \in \mathbb{R}$). We are interested in Santilli's Isonumber Theory of the First Kind, where the new isounit $\hat{I}$ is not in the field. Let the field $F(a, +, .)$ be given (e.g., Z_p, with p prime) and let the isounit $\hat{I} = \hat{T}^{-1} \notin F$ be an invertible quantity. Let a new definition of multiplication be defined on F using $* = \hat{T}$ (see [10]). This allows us to define a new field $\hat{F}(\hat{a}, +, *)$ (called isofield of the first kind), with elements called isonumbers and rules given by:

$$\begin{aligned} &\hat{a} = a\hat{I}, \quad \hat{a} * \hat{b} = (a\hat{I})\hat{T}(b\hat{I}) = ab\hat{I} = \widehat{ab} \\ &\hat{a} + \hat{b} = (a\hat{I}) + (b\hat{I}) = (a+b)\hat{I} = \widehat{a+b}. \\ &\hat{0} = 0\hat{I} = 0 \end{aligned} \tag{2.2}$$

3 The Paillier-Senegalese Algorithm

The construction of the Paillier-Senegalese cryptographic algorithm is accomplished in a three step process. The first step is the generation of

the Paillier-Senegalese public and private isokeys required for encryption and decryption. The second step is the definition and use of the Paillier-Senegalese encryption function with the public isokeys to encrypt each of the pixel intensity value from a given set of R, G, and B-Channel images. The third step is the definition and use of the Paillier Senegalese decryption function with the private isokeys for the decryption phase, recovering the corresponding RGB images.
Let a RGB image be given with an 8-bit encoding for each channel. This means that the pixel intensity values are in the range $[0, (L-1)]$, where is $L = 256$. These pixel intensity values for each channel image can be assumed to belong to the finite prime field $Z_p = \{0, 1, 2, \cdots (p-1)\}$ of order $p = 257$ representing the closest prime number after $L = 256$,
The key generation, encryption and decryption phases are as follows:

3.1 Public and Private Keys Generation

We begin with the use of the Paillier cryptographic system for generating the public and private keys, which we use to generate our Paillier-Senegalese cryptographic system public and private isokeys.

3.1.1 Traditional Paillier public and private keys generation

We randomly choose two large prime numbers q and s, so that the greatest common divisor (gcd) of qs and $(q-1)(s-1)$ is 1, that is

$$gcd(qs, (q-1)(s-1)) = 1. \tag{3.1}$$

The condition is satisfied if q and s are primes with the same length. Our next step is to compute the public key N, and private key λ. This is done by defining $N = q \times s$ and, using the the least common multiple function lcm, to define λ by:

$$\lambda = lcm\,(q-1, s-1)\,. \tag{3.2}$$

To compute the private decryption key μ, we generate a random integer $g \in Z^*_{N^2} = \{1, 2, \ldots, (N^2-1)\}$ such that the order l, of g is a multiple of N.

The value of g can be also computed as $g = 1 + N$ when p and s have the same length. The private decryption key μ is then defined using the modulo operator mod , by:

$$\mu = \{[L(g^{\lambda} \mod (N^2))]^{-1}\} \mod (N), \tag{3.3}$$

where $L[U] = (U - 1)\, N^{-1}$. Hence, the privation key needed for decryption is (λ, μ), while the public key needed for encryption is (N, g).

3.1.2 Paillier-Senegalese Cryptographic System Public and Private keys Generation

The public and private isokeys for the Paillier-Senegalese cryptographic scheme are described in this section. First, we randomly generate two large prime numbers q and s, and randomly generate the isounit $\hat{I}$ outside Z_p. For proof of concept, we have randomly generated the 200 digit integer
$\hat{I} = 91446193624825680120842585289199005703827325309092129$
$49839374420736133837169556773178863114789569739152008171393562 0$
$65024462982808290015616340499507514219090543595507822577096302$
$248569953483357402576 7.$
We use it to compute the following parameters:

$$\hat{q} = q\hat{I} \tag{3.4}$$

$$\hat{s} = s\hat{I} \tag{3.5}$$

$$\hat{N} = \hat{q} * \hat{s} = q\hat{I}\left(\hat{I}^{-1}\right) s\hat{I} = (qs)\hat{I} = N\hat{I} \tag{3.6}$$

Given $\hat{N}$, the value of N can be computed as $N = \hat{N}/\hat{I}$. We can also compute $\hat{N}^{\hat{2}}$ needed for the encryption function using the isomultiplicative operation of the first kind $\hat{a}^{\hat{b}} = a^b\hat{I}$ as follows:

$$\hat{N}^{\hat{2}} = N^2\hat{I} \tag{3.7}$$

The values for $\hat{g}$ and $\hat{p}$ corresponding to g and p are given by

$$\hat{g} = \hat{I} + \hat{N} = \hat{I} + N\hat{I} = (1 + N)\hat{I} = g\hat{I} \tag{3.8}$$

$$\hat{p} = p\hat{I} \tag{3.9}$$

Note that given $\hat{g}$, the value of g can be computed as $g = \hat{g}/\hat{I}$. The function $L(U)$ becomes

$$\begin{aligned} L[\hat{U}] &= \left(\hat{U} - \hat{I}\right) * \hat{N}^{-1} = (U-1)\,\hat{I}(\hat{I}^{-1})\hat{I}N^{-1} \\ &= \left[(U-1)\,N^{-1}\right]\hat{I} = L[U]\hat{I}, \end{aligned} \tag{3.10}$$

The private decryption isokeys corresponding to μ and λ becomes

$$\hat{\mu} = \mu\hat{I} \tag{3.11}$$

$$\hat{\lambda} = lcm(\hat{q} - \hat{I}, \hat{s} - \hat{I}) \tag{3.12}$$

The private isokey $\hat{\lambda}$ is also given by

$$\hat{\lambda} = \lambda\hat{I} \tag{3.13}$$

When $\hat{\lambda}$ is known, λ can be obtained by $\lambda = \hat{\lambda}/\hat{I}$.
Hence, the pairs of public encryption isokey and private decryption isokey are $(\hat{g}, \hat{N})$ and $(\hat{\lambda}, \hat{\mu})$, respectively.

3.2 Paillier-Senegalese RGB Image Encryption Phase

This subsection introduces the traditional Paillier encryption scheme and the modification leading to the Paillier-Senegalese scheme for a given RGB image.
For the traditional Paillier encryption phase, let y_R, y_G, and y_B represent the pixel intensity values for the R, G, and B-channel images respectively. To encrypt each pixel intensity value in the Paillier scheme, one writes:

$$E(y_R) = g^{y_R}x_1^N \mod (N^2) \tag{3.14}$$

$$E(y_G) = g^{y_G}x_2^N \mod (N^2) \tag{3.15}$$

$$E(y_B) = g^{y_B}x_3^N \mod (N^2) \tag{3.16}$$

where $x_i, i = 1, 2, 3$ is a random number in
$Z_N^* = \{1, 2, \ldots, (N-1)\}$. The encrypted values $E(y_R)$, $E(y_G)$, and $E(y_B)$ are outside of our range of $[0, (L-1)]$. To map them back into this range, we apply the mod $[p]$ operation, where p is 257. These values belong to the encrypted channel images that can be transmitted or stored as described in [18], and can be computed as follows:

$$C_R = E(y_R) \mod (p) = \{[g^{y_R} x_1^N \mod (N^2)]\} \mod (p) \tag{3.17}$$

$$C_G = E(y_G) \mod (p) = \{[g^{y_G} x_2^N \mod (N^2)]\} \mod (p) \tag{3.18}$$

$$C_B = E(y_B) \mod (p) = \{[g^{y_B} x_3^N \mod (N^2)]\} \mod (p) \tag{3.19}$$

3.2.1 The Paillier-Senegalese Encryption Scheme

To obtain the Paillier-Senegalese encryption scheme, we replace the above equations by:

$$E(\hat{y}_R) = \hat{g}^{\hat{y}_R} * \hat{x}_1^{\hat{N}} mod(\hat{N}^{\hat{2}}) \tag{3.20}$$

$$E(\hat{y}_G) = \hat{g}^{\hat{y}_G} * \hat{x}_2^{\hat{N}} mod(\hat{N}^{\hat{2}}) \tag{3.21}$$

$$E(\hat{y}_B) = \hat{g}^{\hat{y}_B} * \hat{x}_3^{\hat{N}} mod(\hat{N}^{\hat{2}}) \tag{3.22}$$

where $\hat{x}_i = x_i \hat{I}, i = 1, 2, 3$ is a random isonumber in $\hat{Z}_N^*$, $\hat{g} = g\hat{I}$, etc. (see section 3.1).

Proposition 3.1. *Using the Paillier-Senegalese cryptographic system, we have*

$$E(\hat{y}) = E(y)\hat{I} \tag{3.23}$$

Proof. To encrypt y using Paillier encryption function, we can write

$$E(y) = g^y x^N \mod (N^2) \tag{3.24}$$

Let N^2 be a positive integer and $g^y x^N$ be a nonnegative integer. Using the division algorithm, we have

$$g^y x^N = qN^2 + E(y) \tag{3.25}$$

where $q = \lfloor \frac{g^y x^N}{N^2} \rfloor$, $0 \leq E(y) < N^2$,
where the symbol $\lfloor x \rfloor$ is the floor function which represents the largest integer less than or equal to x.
So using Eq. 3.25, Eq. 3.24 can be written as

$$E(y) = g^y x^N - \lfloor \frac{g^y x^N}{N^2} \rfloor \times N^2 \tag{3.26}$$

Multiplying both side of of Eq. 3.26 by $\hat{I}$ gives

$$E(y)\hat{I} = \left(g^y x^N - \lfloor \frac{g^y x^N}{N^2} \rfloor N^2 \right) \hat{I} \tag{3.27}$$

The right side of Eq. 3.23 can be written as

$$E(\hat{y}) = \hat{g}^{(\hat{y})} * \hat{x}^{(\hat{N})} \mod \hat{N}^{\hat{2}} \tag{3.28a}$$

$$= \left(g^{(y)} x^N \right) \hat{I} \mod (N^2 \hat{I}) \tag{3.28b}$$

$$= \left(g^{(y)} x^N \right) \hat{I} - \lfloor \frac{g^y x^N \hat{I}}{N^2 \hat{I}} \rfloor (N^2 \hat{I}) \tag{3.28c}$$

$$= \left[\left(g^{(y)} x^N \right) - \lfloor \frac{g^y x^N}{N^2} \rfloor N^2 \right] \hat{I} \tag{3.28d}$$

$$E(\hat{y}) = E(y)\hat{I} \tag{3.28e}$$

□

Using the result obtained from Eq. 3.28e, Eqs. 3.20 3.21, and 3.22 can be written as

$$E(\hat{y}_R) = E(y_R)\hat{I} \tag{3.29}$$

$$E(\hat{y}_G) = E(y_G)\hat{I} \tag{3.30}$$

$$E(\hat{y}_B) = E(y_B)\hat{I} \tag{3.31}$$

The computational cost of implementing Eqs. 3.29, 3.30, and 3.31 is less than the computational cost of Eqs. 3.20, 3.21, and 3.22.
Similar to the encryption of RGB images using the traditional Paillier encryption system as described on our previous papers [17], [18] the quantities

$E(\hat{y}_R)$, $E(\hat{y}_G)$, and $E(\hat{y}_B)$ are out of the range $[0,(L-1)]$. They must be mapped to this range by applying mod p to each as follows:

$$\hat{C}_R = E(\hat{y}_R) \mod (p) = [\hat{g}^{(\hat{y}_R)} * \hat{x}_1^{(\hat{N})} \mod (\hat{N})^{\hat{2}}] \mod (p) \tag{3.32}$$

$$\hat{C}_G = E(\hat{y}_G) \mod (p) = [\hat{g}^{(\hat{y}_G)} * \hat{x}_2^{(\hat{N})} \mod (\hat{N})^{\hat{2}}] \mod (p) \tag{3.33}$$

$$\hat{C}_B = E(\hat{y}_B) \mod (p) = [\hat{g}^{(\hat{y}_B)} * \hat{x}_3^{(\hat{N})} \mod (\hat{N})^{\hat{2}}] \mod (p) \tag{3.34}$$

The quantities $\hat{C}_R$, $\hat{C}_G$, and $\hat{C}_B$ represents the encrypted pixel intensity values that will be transmitted and/or stored.
Other parameter needed for the decryption are also computed as follows:

$$q_R = \left\lfloor \frac{E(\hat{y}_R)}{p} \right\rfloor \tag{3.35}$$

$$q_G = \left\lfloor \frac{E(\hat{y}_G)}{p} \right\rfloor \tag{3.36}$$

$$q_B = \left\lfloor \frac{E(\hat{y}_B)}{p} \right\rfloor \tag{3.37}$$

where the symbol $\lfloor\ \rfloor$ represents the floor function. The quantities given in Eqs. (3.35), (3.36), and (3.37) are not secret but can also be encrypted using other encryption methods to increase the security of the cipher images.

3.3 Paillier-Senegalese RGB Image Decryption Phase

This subsection presents the Traditional Paillier Cryptographic Decryption Approach and the Proposed Paillier-Senegalese Cryptographic Decryption Approach.

In our previous paper [17], the traditional Paillier Cryptographic scheme was used for the decryption of $E(y_R)$, $E(y_G,)$ and $E(y_B)$ to obtain y_R, y_G , and y_B.
In particular the encrypted pixel intensity values C_R, C_G, and C_B, and the quotients given by $qt_R = \left\lfloor \frac{E(y_R)}{p} \right\rfloor$, $qt_G = \left\lfloor \frac{E(y_G)}{p} \right\rfloor$, $qt_B = \left\lfloor \frac{E(y_B)}{p} \right\rfloor$ are

assumed available to the decryption function at the receiver side. To reconstruct $E(y_R)$, $E(y_G)$, and $E(y_B)$ before applying the Paillier decryption function, we can write.

$$E(y_R) = qt_R \times p + C_R = \alpha \tag{3.38}$$

$$E(y_G) = qt_G \times p + C_G = \beta \tag{3.39}$$

$$E(y_B) = qt_B \times p + C_B = \gamma \tag{3.40}$$

To recover the original pixels' intensity values y_R, y_G, and y_B, the Paillier decryption function is applied to $E(y_R) = \alpha$, $E(y_G) = \beta$, and $E(y_B) = \gamma$ in Eqs. (3.38), (3.39), and (3.40) as follows:

$$y_R = \frac{L[\alpha^\lambda \mod (N^2)]}{L[g^\lambda \mod (N^2)]} \mod (N) \tag{3.41}$$

$$y_G = \frac{L[\beta^\lambda \mod (N^2)]}{L[g^\lambda \mod (N^2)]} \mod (N) \tag{3.42}$$

$$y_B = \frac{L[\gamma^\lambda \mod (N^2)]}{L[g^\lambda \mod (N^2)]} \mod (N) \tag{3.43}$$

3.3.1 The Paillier-Senegalese Decryption Approach

Now, consider our proposed Paillier-Senegalese decryption method. Assume that the quantities q_R, q_G, and q_B are available to the decryption function in addition to $\hat{C}_R$, $\hat{C}_G$, and $\hat{C}_B$.
One must first reconstruct $E(\hat{y}_R)$, $E(\hat{y}_G)$, and $E(\hat{y}_B)$ from the receive cipher pixel values, $\hat{C}_R$, $\hat{C}_G$, and $\hat{C}_B$ before applying the decryption function as follows.

$$E(\hat{y}_R) = q_R \times p + \hat{C}_R = \hat{\alpha} \tag{3.44}$$

$$E(\hat{y}_G) = q_G \times p + \hat{C}_G = \hat{\beta} \tag{3.45}$$

$$E(\hat{y}_B) = q_B \times p + \hat{C}_B = \hat{\gamma} \tag{3.46}$$

The Paillier-Senegalese decryption function can be applied to $E(\hat{y}_R)$, $E(\hat{y}_G)$, and $E(\hat{y}_B)$, in Eqs. (3.44), (3.45), and (3.46) to recover the original

pixels' intensity values $\hat{y}_R$, $\hat{y}_G$, and $\hat{y}_B$, and then y_R, y_G, and y_B belonging to our original channel images. They are computed as follows:

$$\hat{y}_R = \frac{L[\hat{\alpha}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})]}{L[\hat{g}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})]} \mod (\hat{N}) \tag{3.47}$$

$$\hat{y}_G = \frac{L[\hat{\beta}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})]}{L[\hat{g}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})]} \mod (\hat{N}) \tag{3.48}$$

$$\hat{y}_B = \frac{L[\hat{\gamma}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})]}{L[\hat{g}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})]} \mod (\hat{N}) \tag{3.49}$$

From equations 3.11 and 3.3, $L[\hat{g}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})] = \hat{\mu} = \mu\hat{I}$, so that these equations can be written as:

$$\hat{y}_R = \left\{ L[\hat{\alpha}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})] * \hat{\mu} \right\} \mod (\hat{N}) \tag{3.50}$$

$$\hat{y}_G = \left\{ L[\hat{\beta}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})] * \hat{\mu} \right\} \mod (\hat{N}) \tag{3.51}$$

$$\hat{y}_B = \left\{ L[\hat{\gamma}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})] * \hat{\mu} \right\} \mod (\hat{N}) \tag{3.52}$$

To find $L[\hat{\alpha}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})]$, let $\hat{U} = \hat{\alpha}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})$. The value of $\hat{U}$ can also be computed as $\hat{U} = (\alpha^{\lambda})\hat{I} \mod (\hat{N}^{\hat{2}})$ and using Eq. 3.10 we have

$$L[\hat{\alpha}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})] = L(\hat{U}) = \frac{(\hat{U} - \hat{I})}{N} \tag{3.53}$$

Another method of computing $L[\hat{\alpha}^{\hat{\lambda}} mod(\hat{N}^{\hat{2}})]$ is given by

$$L[\hat{\alpha}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})] = L(\hat{U}) = L(U)\hat{I} \tag{3.54}$$

where $L(U)$ is given in section 3.1.1 and $U = \alpha^{\lambda} mod N^2$, where $\alpha = \frac{\hat{\alpha}}{\hat{I}}$.
Similarly, let $\hat{U}_1 = \hat{g}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})$. The expression of $\hat{U}_1$ can also be written as $\hat{U}_1 = (g^{\lambda})\hat{I} mod(\hat{N}^{\hat{2}})$ and we can also write

$$L[\hat{g}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})] = L(\hat{U}_1) = \frac{(\hat{U}_1 - \hat{I})}{N} \tag{3.55}$$

Furthermore, Eq. 3.55 is also given by

$$L[\hat{g}^{\hat{\lambda}} \mod (\hat{N}^{\hat{2}})] = L(\hat{U}_1) = L(U_1)\hat{I} \tag{3.56}$$

where $L(U_1)$ is given in section 3.1.1 and $U_1 = g^{\lambda} \mod (N^2)$.
Similar analysis from Eq. 3.50 through Eq. 3.56 can be also apply to further compute the values of $\hat{y}_G$ and $\hat{y}_B$ in Eqs. 3.48 and 3.49. Now, the values of y_R, y_G, and y_B are given by

$$y_R = \frac{\hat{y}_R}{\hat{I}}, \quad y_G = \frac{\hat{y}_G}{\hat{I}}, \quad y_B = \frac{\hat{y}_B}{\hat{I}} \tag{3.57}$$

For software implementation purposes, it is more efficient to use matrices of pixels' intensity values instead of individual pixels.

4 CONCLUSION

In this paper, we have introduced the Paillier-Senegalese cryptographic scheme which combines the Santilli's Isonumber Theory of the first kind with the Paillier Cryptographic System to provide an additional degree of freedom to the encryption-decryption of RGB images. This leads to a Hybrid public private-key cryptographic system with a substantial increase in image security, which also may be used in a variety of applications for secure systems that may not be related to image encryption and decryption.

References

[1] A. Soleymani, Md. J. Nordin, and Z. Md. Ali, *A Novel Public Key Image Encryption Based on Elliptic Curves over Prime Group Field*, Journal of Image and Graphics, Vol. 1, No. 1, March, 2013.

[2] A. Kanso, M. Ghebleh, *A novel image encryption algorithm based on a 3D chaotic map*, Commun Nonlinear Sci Numer Simulat 17 (2012) 2943–2959,
`www.elsevier.com/locate/cnsns`

[3] A. Daneshgar and B. Khadem, *A self-synchronized chaotic image encryption scheme*, Signal Processing: Image Communication 36 (2015) 106-114.
`www.elsevier.com/local/image`

[4] A. K. A. Hassan, *Reliable Implementation of Paillier Cryptosystem*, Iraqi Journal of Applied Physics, IJAP, Vol. 10, No. 4, October-December 2014, pp. 27-29

[5] R. M.Santilli-1, *Foundations of Theoretical Mechanics II*, Springer-Verlag New York, U.S.A, (1978), ISBN 0-387-08874-1.

[6] R. M.Santilli-2, *Isonumbers and Genonumbers of Dimensions 1, 2, 4, 8, their Isoduals and Pseudoduals, and "Hidden Numbers," of Dimension 3, 5, 6, 7*, Algebras, Groups and Geometries, Vol. 10, 273 (1993).

[7] R. M.Santilli-3, *Elements of Hadronic Mechanics I*, Ukraine Academy of Sciences, Kiev, (1995), Ukraine, ISBN 0-911767-68-1.

[8] R. M.Santilli-4, *Isorepresentation of the Lie-isotopic SU(2) Algebra with Application to Nuclear Physics and Local Realism*, Acta Applicandae Mathematicae Vol. 50, 177 (1998).

[9] C. Corda, *Introduction to Santilli's IsoNumbers*, AIP Conf. Proceed. 1479, 1013 (2012),

[10] C. X. Jiang, *Foundations of Santilli's Isonumber Theory*, Fundamental Open Problems in Science at the End of the Millennium, Proceeding of the Beijing Workshop, August 1997, Hadronic Press, Palm Harbor, FL 34682-1577, U.S.A, ISBN 1-57485-029-6, PP. 105-139, Edited by Tepper Gill (Co-author of this paper), K. Liu, and E. Trell.

[11] G. Zhang, and Q. Liu, *A novel image encryption method based on total shuffling scheme*, Optics Communications 284 (2011) 2775–2780, www.elsevier.com/locate/optcom

[12] G. Chen, Y. Mao, and C. K. Chui, *A symmetric image encryption scheme based on 3D chaotic cat maps*, Chaos, Solitons and Fractals 21 (2004) 749–761, www.elsevier.com/locate/chaos

[13] G. Ye and X. Huang, *An Image Encryption Algorithm Based on Autoblocking and Electrocardiography*, Published by the IEEE Computer Society. April-June 2016.

[14] H. Liu, X. Wang, and A. kadir, *Image encryption using DNA complementary rule and chaotic maps*, Applied Soft Computing 12 (2012) 1457–1466, www.elsevier.com

[15] H. S. Kwok, Wallace K. S. Tang, *A fast image encryption system based on chaotic maps with finite precision representation*, Chaos, Solitons and Fractals 32 (2007) 1518–1529, www.elsevier.com/locate/chaos

[16] L. D. Singh and K. M. Singh, *Image Encryption using Elliptic Curve Cryptography*, Procedia Science 54 (2015) 475-481, www.sciencedirect.com

[17] M. I. Wade, H. C. Ogworonjo, M. Gul, M. Ndoye, M. Chouikha, W. Paterson *Red Green Blue Image Encryption Based on Paillier Cryptographic Cryptographic Approach*, World Academy of Science, Engineering and Technology, International Journal of Electronics and Commu-

nication Engineering Vol:11, No:12, 2017,
https://waset.org/abstracts/79232

[18] M. I. Wade, *Distributed Image Encryption Based On a Homomorphic Cryptographic Approach*, 10th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, Columbia University, New York City, USA 10- 12 October 2019 (IEEE UEMCON 2019).

[19] N. K. Pareek, V. Patidar, and K. K. Sud, *Image Encryption Using Chaotic Logistic Map*, Image and Vision Computing 24 (2006) 926-934,
www.elsevier.com/locate/optlaseng

[20] P. P. Dang and P. M. Chau, *Image Encryption for Secure Internet Multimedia Applications*, IEEE Trans. On Consumer Electronics, Vol. 46. No. 3, August 2000.

[21] R. Tao, X. Meng, and Y. Wang, *Image Encryption With Multiorders of Fractional Fourier Transforms*, IEEE Trans. Inf. Forensics and Security, Vol. 5, No 4, Dec 2010.

[22] R. Rivest, Lecture Notes 15, Computer and Network Security: *Voting, Homomorphic Encryption*, October, 2002

[23] R. C. Gonzalez and R. E. Woods, *Digital Image Processing.*,3rd ed. Person Education Inc., 2008.

[24] R. Rhouma, S. Meherzi, and S. Belghith, *OCML-based colour image encryption*, Chaos, Solitons and Fractals 40 (2009) 309–318,
www.elsevier.com/locate/chaos

[25] S. Mazloom and A. M. E-Moghadam, *Color image encryption based on Coupled Nonlinear Chaotic Map*, Chaos, Solitons and Fractals 42 (2009) 1745–1754,
www.elsevier.com/locate/chaos

[26] *University of Southern California, Signal and Image Processing Institute*,
http://sipi.usc.edu/database/

[27] Y. Zhou, L. Bao, C. L. P. Chen *A new 1D chaotic system for image encryption*, Signal Processing 97 (2014) 172–182, www.elsevier.com/locate/sigpro

[28] Yi. Xun, P. Russell, and B. Elisa, *Homomorphic Encryption and Applications*, 2014 XII, 126 p. 23 illus., http://www.springer.com/978-3-319-12228-1

ALGEBRAS GROUPS AND GEOMETRIES 35 413 - 426 (2018)
DOI 10.29083/AGG.35.04.2018

ON EXTENDED CAMPOPIANO'S TYPE BOUND FOR LPA CODES

Sapna Jain
Shanxi Normal University
P. R. China
sapnajain@gmx.com

K. P. Shum
Institute of Mathematics, Yunnan University
Kunming, 650091
P. R. China
kpshum@ynu.edu.cn

Received February 7, 2020
Revised June 17, 2020

Abstract

Linear partition Arihant (LPA) codes have been introduced by the author in [3] and a study of error correcting/detecting capabilities of these code was made with respect to the random block errors [2]. Also, the concept of P-bursts has been formulated by the author in [5] to study clustered block errors that occur during the process of communication. In this paper, we take up the problem of simultaneous correction of P-burst errors with the detection of random block errors in LPA codes and obtain an extended Campopiano's type bound for LPA codes.

Keywords: LPA codes, LPA distance, P-bursts

Copyright © 2018 by Hadronic Press Inc., Palm Harbor, FL 34682, U.S.A.

1. Introduction

P-burst error correcting/detecting codes [5] are suitable for correcting/detecting block errors which do not occur independently but are clustered over a particular block length. These type of errors occur in many situations. One important and practical situation is in which the transmitted/stored information is disturbed over a particular block length together with occasional disturbances, thus, creating simultaneously P-bursts as well as random block errors. Such a situation arise, e.g., in semiconductor memory systems where the memory is highly vulnerable to clustered block errors due to bombardment of strong radioactive particles such as cosmic particles on RAM chips and occasional/random block errors result from decay of RAM chips. However, P-burst error correcting LPA codes fail to detect even a few random block errors when these are not within P-bursts of specified block length. Under such type of situations, block codes capable of correcting P-burst errors and simultaneously detecting random block errors are very useful. Keeping this in view, in this paper, we obtain a construction upper bound on the number of parity check digits required for LPA codes correcting weighted P-burst block errors and simultaneously detecting random block errors of upto a specified Arihant weight. The bound obtained in this paper is an extended Campopiano's type bound [1] for LPA block space.

2. Preliminaries

Let q, n be positive integers with $q > 1$. Let $\mathbf{Z}_q$ be the ring of integers modulo q. Let $\mathbf{Z}_q^n$ be the set of all n-tuples over $\mathbf{Z}_q$. Then $\mathbf{Z}_q^n$ is a module over $\mathbf{Z}_q$. For q prime, $\mathbf{Z}_q$ becomes a field and $\mathbf{Z}_q^n$ becomes a vector space over $\mathbf{Z}_q$. A partition P of the positive integer n is defined as

$$\begin{aligned} P \quad : \quad & n = n_1 + n_2 \cdots + n_s \quad \text{where} \\ & 1 \leq n_1 \leq n_2 \leq \cdots \leq n_s, s \geq 1. \end{aligned}$$

The partition P is denoted as

$$P : n = [n_1][n_2] \cdots [n_s].$$

In the case, when

$$\begin{aligned} P : n \quad = \quad & \underbrace{[m_1] \cdots [m_1]}_{l_1\text{- copies}} \underbrace{[m_2] \cdots [m_2]}_{l_2\text{- copies}} \\ & \cdots \underbrace{[m_r] \cdots [m_r]}_{l_r\text{- copies}}, \end{aligned}$$

we write

$$P : n = [m_1]^{l_1}[m_2]^{l_2} \cdots [m_r]^{l_r},$$

where $m_1 < m_2 < \cdots < m_r$.

Given a partition $P : n = [n_1][n_2] \cdots [n_s]$ of the positive integer n, the module space $\mathbf{Z}_q^n$ over $\mathbf{Z}_q$ can be viewed as a direct sum

$$\begin{aligned} \mathbf{Z}_q^n &= \mathbf{Z}_q^{n_1} \oplus \mathbf{Z}_q^{n_2} \oplus \cdots \oplus \mathbf{Z}_q^{ns}, \\ &\text{or} \\ V &= V_1 \oplus V_2 \oplus \cdots V_s, \end{aligned}$$

where $V = \mathbf{Z}_q^n$ and $V_i = \mathbf{Z}_q^{n_1}$ for all $1 \leq i \leq s$.

Consequently, each vector $v \in \mathbf{Z}_q^n$ can be uniquely written as $v = (v_1, v_2, \cdots, v_s)$ where $v_i \in V_i = \mathbf{Z}_q^{n_i}$ for all $1 \leq i \leq s$.

Here $v_i (1 \leq i \leq s)$ is called the i^{th} *block of block size* n_i of the vector v.

Further, we define the modular value $|a|$ of an element $a \in \mathbf{Z}_q$ by

$$|a| = \begin{cases} a & \text{if} \quad 0 \leq a \leq q/2 \\ q - a & \text{if} \quad q/2 < a \leq q - 1. \end{cases}$$

We note that non-zero modular value $|a|$ can be obtained by two different elements viz. a and $q - a$ of $\mathbf{Z}_q$ provided $\{q$ is odd$\}$ or $\{q$ is even and $a \neq [q/2]\}$ i.e.

$$|a| = |q - a| \quad \text{if} \quad \begin{cases} q \text{ is odd} \\ \text{or} \\ q \text{ is even and } a \neq q/2. \end{cases}$$

If q is even and $a = [q/2]$ or if $a = 0$, then $|a|$ is obtained in only one way viz. $|a| = a$. Thus there may be one or two equivalent values of $|a|$ which we shall refer to as repetitive equivalent values of a. The number of repetitive equivalent values of a will be denoted by e_a where

$$e_a = \begin{cases} 1 & \text{if } \{ q \text{ is even and } a = [q/2]\} \text{ or } \{a = 0\} \\ 2 & \text{if } \{ q \text{ is odd and } a \neq 0\} \text{ or } \{q \text{ is even, } a \neq 0 \text{ and } a \neq [q/2]\}. \end{cases}$$

3. Definitions and notations

We begin with the discussion of LPA codes [3]:

Let n, q be positive integers with $q > 1$. Let $P : n = [n_1][n_2]\cdots[n_s]$ be a partition of n. We define *Arihant metric* on $\mathbf{Z}_q^n$ corresponding to the partition P as follows:

Let $v = (v_1, v_2, \cdots, v_s) \in \mathbf{Z}_q^n = \mathbf{Z}_q^{n_1} \oplus \mathbf{Z}_q^{n_2} \oplus \cdots \oplus \mathbf{Z}_q^{n_s}$. The Arihant weight of the i^{th} block $v_i \in \mathbf{Z}_q^{n_i} (1 \leq i \leq s)$ of the vector v corresponding to the partition P of n is defined as

$$w_A^P(v_i) = \max_{j=1}^{n_i} |v_j^{(i)}|$$

where

$$v_i \quad = \quad (v_1^{(i)}, v_2^{(i)}, \cdots, v_{n_i}^{(i)}) \in \mathbf{Z}_q^{n_i}.$$

Thus the Arihant weight of a block is the maximum modular value amongst all its components. Then the Arihant weight of the vector $v = (v_1, v_2, \cdots, v_s) \in \mathbf{Z}_q^{n_1} \oplus \mathbf{Z}_q^{n_2} \oplus \cdots \oplus \mathbf{Z}_q^{n_s}$ corresponding to the partition P is defined as the sum of Arihant weights of all its blocks i.e.

$$W_A^P(v) = \sum_{i=1}^{s} w_A^P(v_i).$$

For any $u = (u_1, u_2, \cdots, u_s)$ and $v = (v_1, v_2, \cdots, v_s) \in \mathbf{Z}_q^n = \mathbf{Z}_q^{n_1} \oplus \mathbf{Z}_q^{n_2} \oplus \cdots \oplus \mathbf{Z}_q^{n_s}$, we define the Arihant distance (or Arihant metric) $d_A^P(u, v)$ between u and v as

$$d_A^P(u, v) = w_A^P(u - v).$$

Then d_A^P is a metric on $\mathbf{Z}_q^n = \mathbf{Z}_q^{n_1} \oplus \cdots \oplus \mathbf{Z}_q^{n_s}$.

If the partition P is clear from the context, we shall denote Arihant weight by w_A and Arihant metric by d_A only.

Definition 3.1 [3]. A linear partition Arihant (LPA) code corresponding to the partition $P : n = [n_1]\cdots[n_s]$ is a $\mathbf{Z}_q$-submodule of $\mathbf{Z}_q^n = \mathbf{Z}_q^{n_1} \oplus \mathbf{Z}_q^{n_2} \oplus \cdots \oplus \mathbf{Z}_q^{n_s}$ equipped with the Arihant metric and is denoted as $[n, k, d_A; P]$ or $[n, k; P]$ code where

$$k = \text{rank}_{\mathbf{Z}_q}(V),$$

and

$$\begin{aligned} d_A &= d_A(V) \\ &= \text{minimum Arihant distance of } V \\ &= \min\{d_A(u, u') \mid u, u' \in V,\ u \neq u'\}. \end{aligned}$$

Remark 3.2.

1. For $P : n = [1]^n$, the linear partition Arihant codes reduce to the classical Lee weight codes [7-9]. For this partition, the Arihant distance and Arihant weight reduce to classical Lee distance and Lee weight respectively.

2. For $q = 2, 3$, the linear partition Arihant codes reduce to the linear error-block codes [1] and the Arihant metric reduces to the π-metric introduced by Feng et al. [2].

3. In general, we have

$$\begin{aligned} \pi\text{-metric} &\leq \text{Arihant metric} \\ &\leq \text{Lee metric,} \end{aligned}$$

or equivalently

$$\begin{aligned} \pi\text{-weight} &\leq \text{Arihant weight} \\ &\leq \text{Lee weight.} \end{aligned}$$

We now define P-burst in $\mathbf{Z}_q^n = \mathbf{Z}_q^{n_1} \oplus \mathbf{Z}_q^{n_2} \oplus \cdots \oplus \mathbf{Z}_q^{n_s}$ as follows [5].

Definition 3.3 [5]. Let n be a positive integers and $P : n = [n_1][n_2]\cdots[n_s]$, $1 \leq n_1 \leq n_2 \leq \cdots \leq n_s$ be a partition of n. A P-burst of block length b $(1 \leq b \leq s)$ is a vector $v = (v_1, v_2, \cdots, v_s) \in \mathbf{Z}_q^n = \bigoplus_{i=1}^{s} \mathbf{Z}_q^{n_i}$ such that all the non-zero blocks in v are confined to some b consecutive block positions, the first and last of which are non-zero.

Definition 3.4 [5]. A P-burst of block length b or less $(1 \leq b \leq s)$ is a P-burst of block length t where $1 \leq t \leq b \leq s$.

Throughout this paper, we shall use the following notations:

1. $[x]$ = The largest integer less than or equal to x.

2. $\lceil x \rceil$ = The smallest integer greater than or equal to x.

3. Q_i=The sum of repetitive equivalent values up to i i.e.,

$$Q_i = e_0 + e_1 + \cdots + e_i$$

where e_i denotes the repetitive equivalent value of i.

4. Extended Campopiano's type bound for LPA codes correcting P-burst errors and simultaneously detecting random block errors

In this section, we obtain an extended Campopiano's type bound which is infact a sufficient bound on the number of parity checks required for an LPA code that correct all random block errors of Arihant weight t or less ($t \geq 1$) and simultaneously detect all P burst errors of block length b or less ($b \geq 1$) with Arihant weight w or less ($w \geq t$).

To prove the result, we need the following.

Let $A_{t,q}^{(n_1,n_2,\cdots,n_s)}$ [6] denote the number of all n-vectors corresponding to the partition $P : n = [n_1][n_2]\cdots[n_s]$ with $1 \leq n_1 \leq n_2 \leq \cdots \leq n_s$ having Arihant weight t over $\mathbf{Z}_q$. Then $A_{t,q}^{(n_1,n_2,\cdots,n_s)}$ is given by :

$$A_{t,q}^{(n_1,n_2,\cdots,n_s)} = \sum_{r=(r_{ij})} \left(\prod_{i=1}^{s} \prod_{j=0}^{[q/2]} ((Q_j)^{n_i} - (Q_{j-1})^{n_i})^{r_{ij}} \right), \tag{1}$$

where $r = (r_{ij})(1 \leq i \leq s, 0 \leq j \leq [q/2]$ satisfies

(i) for a fixed $i(1 \leq i \leq s), r_{ij} = 1$ for exactly one value of $j(0 \leq j \leq [q/2])$ and 0 elsewhere; and

(ii)

$$\sum_{i=1}^{s} \sum_{j=0}^{[q/2]} j r_{ij} = t. \tag{2}$$

Again if $V_{t,q}^{(n_1,n_2,\cdots,n_s)}$ denote the number of all n-vector corresponding to the partition $P : n = [n_1][n_2]\cdots[n_s], 1 \leq n_1 \leq n_2 \leq \cdots \leq n_s$ having Arihant weight t or less over $\mathbf{Z}_q$. Then $V_{t,q}^{(n_1,n_2,\cdots,n_s)}$ is given by

$$V_{t,q}^{(n_1,n_2,\cdots,n_s)} = \sum_{j=0}^{t} A_{t,q}^{(n_1,n_2,\cdots,n_s)} \tag{3}$$

We now give a definition for linear combination of vectors having Arihant weight w.

Definition 4.1. A linear combination of vectors $u_1, u_2, \cdots, u_r$ given by

$$\lambda_1.u_1 + \lambda_2.u_2 + \cdots + \lambda_r.u_r,$$

where $\lambda_i = (\lambda_1^{(i)}, \lambda_2^{(i)} \cdots \lambda_{n_i}^{(i)}), u_i = (u_1^{(i)}, u_2^{(i)}, \cdots, u_{n_i}^{(i)}) \in \mathbf{Z}_q^{n_i}$ for all $1 \leq i \leq r$ and $(.)$ denote the usual dot product of vectors, is called a linear combination of Arihant weight w if

$$\max_{a=1}^{n_1}|\lambda_a^{(1)}| + \max_{b=1}^{n_2} + |\lambda_b^{(2)}| + \cdots + \max_{l=1}^{n_r}|\lambda_l^{(r)}| = w.$$

The following lemma enumerates the number of Arihant weighted P-bursts in block coding:

Lemma 4.2. The number of P bursts of block length b or less with Arihant weight $g \geq 1$ in the space of all $(n_1 + n_2 + \cdots + n_{j-1})$-block vectors over the ring $\mathbf{Z}_q$ is given by

$$\begin{aligned} C_q(b, \sum_{i=1}^{j-1} n_i, g) &= C_q(1, \sum_{i=1}^{j-1} n_i, g) + \sum_{m=2}^{b}\sum_{r=1}^{j-m}\Bigg(\sum_{\substack{2\leq\lambda_1+\lambda_2\leq g \\ \lambda_1,\lambda_2\geq 1}} ((Q_{\lambda_1})^{n_r} - (Q_{\lambda_1-1})^{n_r}) \times \\ &\quad ((Q_{\lambda_2})^{n_{r+m-1}} - (Q_{\lambda_2-1})^{n_{r+m-1}}) A_{g-\lambda_1-\lambda_2,q}^{(n_{r+1},n_{r+2},\cdots,n_{r+m-2})}\Bigg), \end{aligned} \tag{4}$$

where

$$C_q(1, \sum_{i=1}^{j-1} n_i, g) = \begin{cases} \sum_{i=1}^{j-1}((Q_g)^{n_i} - (Q_{g-1})^{n_i}) & \text{if } g \leq [q/2], \\ 0 \quad \text{if } g > [q/2], \end{cases}$$

and $A_{g-\lambda_1-\lambda_2,q}^{(n_{r+1},n_{r+2},\cdots,n_{r+m-2})}$ is given by (1) satisfying (2).

Proof. There are two cases:

Case 1. When $b = 1$.

In this case, the number of P-bursts of block length 1 with Arihant weight g in the space of all $n_1 + n_2 + \cdots + n_{j-1}$-tuples over $\mathbf{Z}_q$ is given by

$$C_q(1, \sum_{i=1}^{j-1} n_i, g) = \begin{cases} \sum_{i=1}^{j-1}((Q_g)^{n_i} - (Q_{g-1})^{n_i}) & \text{if } g \leq [q/2], \\ 0 \quad \text{if } g > [q/2]. \end{cases} \tag{5}$$

Case 2. When $b \geq 2$.

Consider a P-burst of block length m and Arihant weight g where $2 \leq m \leq b \leq j-1$ and $g \geq 1$. Such a P-burst can have first $(j-m)$ block positions as the starting block positions. Suppose the P-burst starts at the r^{th} block $(1 \leq r \leq j-m)$ and suppose that the Arihant weights of the starting and ending blocks are $\lambda_1(\neq 0)$ and $\lambda_2(\neq 0)$ resp.

Then the number of choices for the starting r^{th} block and ending $(r+m-1)^{th}$ block together is given by

$$((Q_{\lambda_1})^{n_r} - (Q_{\lambda_1-1})^{n_r})((Q_{\lambda_2})^{n_{r+m-1}} - (Q_{\lambda_2-1})^{n_{r+m-1}}). \tag{6}$$

The remaining $(m-2)$ blocks viz $(r+1)^{th}, (r+2)^{th}, \cdots, (r+m-2)^{th}$ blocks of the P-burst should make up a sum of Arihant weight $g-\lambda_1-\lambda_2$ so that the total Arihant weight of the P-burst becomes equal to g. The number of ways in which these $(m-2)$ blocks can be filled is given by

$$A_{g-\lambda_1-\lambda_2,q}^{(n_{r+1},n_{r+2},\cdots,n_{r+m-2})}, \tag{7}$$

where $A_{g-\lambda_1-\lambda_2,q}^{(n_{r+1},n_{r+2},\cdots,n_{r+m-2})}$ is given by (1) satisfying (2).

The total number of P-bursts of Arihant weight g and block length m starting from the r^{th} block is obtained by multiplying (6) and (7) and then summing the resulting product for different values of $\lambda_1's$ and $\lambda_2's$ satisfying $\lambda_1 \geq 1, \lambda_2 \geq 1$, $2 \leq \lambda_1+\lambda_2 \leq g$ and is given by

$$\sum_{\substack{2\leq\lambda_1+\lambda_2\leq g \\ \lambda_1,\lambda_2\geq 1}} ((Q_{\lambda_1})^{n_r} - (Q_{\lambda_1-1})^{n_r})((Q_{\lambda_2})^{n_{r+m-1}} - (Q_{\lambda_2-1})^{n_{r+m-1}}) \times$$
$$A_{g-\lambda_1-\lambda_2,q}^{(n_{r+1},n_{r+2},\cdots,n_{r+m-2})}. \tag{8}$$

Since r can take values from 1 to $j-m$ and m can take values from 2 to b, therefore, summing (8) for different values for m and r gives the number of P-bursts of block length varying from 2 to b and having Arihant weight g and is given by

$$\sum_{m=2}^{b}\sum_{r=1}^{j-m}\Bigg(\sum_{\substack{2\leq\lambda_1+\lambda_2\leq g \\ \lambda_1,\lambda_2\geq 1}} ((Q_{\lambda_1})^{n_r} - (Q_{\lambda_{1-1}}^{n_r}) \times$$
$$((Q_{\lambda_2})^{n_{r+m-1}} - (Q_{\lambda_2-1})^{n_{r+m-1}})A_{g-\lambda_1-\lambda_2,q}^{(n_{r+1},n_{r+2},\cdots,n_{r+m-2})}\Bigg). \tag{9}$$

The result now follows by adding (5) and (9). □

Remark 4.3.(i) The number of all P-bursts in $\mathbf{Z}_q^n = \bigoplus_{i=1}^{s}\mathbf{Z}_q^{n_i}$ of block length b or less $(b \leq s)$ with Arihant weight w or less including the pattern of all zeros is given by

$$C_q^*(b, \sum_{i=1}^{s} n_i, w) = 1 + \sum_{g=1}^{w} C_q(b, \sum_{i=1}^{s} n_i, g).$$

(ii) The number of all P-bursts in $\mathbf{Z}_q^n = \bigoplus_{1=1}^{s} \mathbf{Z}_q^{n_i}$ of block length b or less ($b \leq s$) having Arihant weight lying between w_1 and w_2 is given by

$$C_q^*(b, \sum_{i=1}^{s} n_i, w_1, w_2) = \sum_{g=w_1}^{w_2} C_q(b, \sum_{i=1}^{s} n_i, g).$$

We now prove the extended Campopiano's type bound for LPA codes correcting P-burst errors and simultaneously detecting random block errors.

Theorem 4.4. *Let n be a positive integer and $P : n = [n_1][n_2]\cdots[n_s], 1 \leq n_1 \leq n_2 \leq \cdots \leq n_s$ be a partition of n. Let t, w and b be positive integers such that $1 \leq t \leq 2w \leq 2b[q/2]$ and $s \geq 2b$. Then a sufficient condition for the existence of an $[n, k; P]$ LPA code with minium Arihant weight at least t that correct all P-bursts of block length b or less having Arihant weight w or less is given by*

$$q^{n-k} \geq \left(\sum_{\lambda=1}^{[q/2]} ((Q_\lambda)^{n_s} - (Q_{\lambda-1})^{n_s} \right) \times D + E, \tag{10}$$

where

$$\begin{aligned} D = {} & V_{t-1-\lambda,q}^{(n_1,n_2,\cdots,n_{s-1})} + C_q^*(b-1, \sum_{i=s-b+1}^{s-1} n_i, 2t-\lambda, 2w-\lambda) + \\ & \sum_{k=1}^{b-1} \sum_{\theta=1}^{min([q/2],w-1)} \sum_{r_{1\theta}, r_{2\theta}, r_{3\theta}} ((Q_\theta)^{n_{s-2b+k+1}} - (Q_{\theta-1})^{n_{s-2b+k+1}}) \times \\ & A_{r_{1\theta},q}^{(n_{s-2b+k+1},\cdots,n_{s-b})} A_{r_{2\theta},q}^{(n_{s-b+1},\cdots,n_{s-b+k})} A_{r_{3\theta},q}^{(n_{s-b+k+1},\cdots,n_{s-1})}, \end{aligned}$$

and

$$E = \sum_{\substack{p_1,p_2: \\ p_1+p_2=t}}^{2w} \sum_{\lambda=1}^{[q/2]} ((Q_\lambda)^{n_s} - (Q_{\lambda-1})^{n_s}) A_{p_1-\lambda,q}^{(n_{s-b+1},\cdots,n_{s-1})} C_q(b, \sum_{i=1}^{s-b} n_i, p_2),$$

subject to

$$\begin{aligned} & 1 \leq \theta + r_{1\theta} \leq w-1; \\ & 1 \leq +r_{2\theta} \leq 2w-1-\lambda; \\ & 0 \leq +r_{3\theta} \leq w-\lambda; \\ & r_{2\theta} + r_{3\theta} \geq t-\lambda; \\ & \theta + r_{1\theta} + r_{2\theta} \geq t; \\ & 2t-\lambda \leq \theta + r_{1\theta} + r_{2\theta} + r_{3\theta} \leq 2w-\lambda; \\ & 0 \leq p_1, p_2 \leq w. \end{aligned} \tag{11}$$

Proof. The existence of such a code is shown by constructing an appropriate $(n-k) \times n$ (where $n = n_1 + n_2 + \cdots + n_s$) parity check matrix H for the desired LPA code. The constructed block matrix H will be of the form

$$H = [H_1, H_2, \cdots, H_s],$$

where $H_i = (H_1^{(i)}, H_2^{(i)}, \cdots, H_{n_i}^{(i)})$ is the i^{th} block of H of size n_i.

We construct the block matrix H as follows:

Suppose we have chosen the first $(j-1)$ blocks suitably. The j^{th} block H_j of size n_j can be added to H provided the following two conditions are satisfied:

1. There should not exist a linear dependence relation between blocks of columns of H of Arihant weight $(t-1)$ or less i.e. every linear combination of Arihant weight $(t-1)$ or less of the blocks of columns of H must be linearly independent;

2. Any two linear combinations, each of Arihant weight w or less, of blocks of columns of H from amongst b or fewer consecutive blocks should be different.

In other words, we can say

$$\lambda_1.H_1 + \lambda_2.H_2 + \cdots + \lambda_{j-1}.H_{j-1} + \lambda_j.H_j \neq 0, \tag{12}$$

and

$$\begin{aligned}&(\alpha_j.H_j + \alpha_{j-1}.H_{j-1} + \cdots + \alpha_{j-b+1}.H_{j-b+1}) + \\ &(\beta_{i_1}.H_{i_1} + \beta_{i_2}.H_{i_2} + \cdots + \beta_{i_b}.H_{i_b}) \neq 0,\end{aligned} \tag{13}$$

where

(i) $\lambda_1.H_1+\lambda_2.H_2+\cdots+\lambda_{j-1}.H_{j-1}+\lambda_j.H_j$ ($\lambda_i \in \mathbf{Z}_q^{n_i}$ for all $1 \leq i \leq j-1, \lambda_j \in \mathbf{Z}_q^{n_j}/\{0\}$ is any linear combination of the j^{th} block H_j to be added and the first $(j-1)$ previously chosen blocks such that the Arihant weight of the linear combination is atmost $t-1$;

(ii) $\alpha_j.H_j + \alpha_{j-1}.H_{j-1} + \cdots + \alpha_{j-b+1}.H_{j-b+1}$ ($\alpha_i \in \mathbf{Z}_q^{n_i}$ for all $j-b+1 \leq i \leq j-1$ and $\alpha_j \in \mathbf{Z}_q^{n_j}/\{0\}$ is any linear combination of Arihant weight w or less of the blocks of columns from amongst the j^{th} block H_j to be added and the immediately preceding $(b-1)$ blocks;

(iii) $\beta_{i_1}.H_{i_1}+\beta_{i_2}.H_{i_1}+\cdots+\beta_{i_b}.H_{i_b}$ ($\beta_l \in \mathbf{Z}_q^{n_l}$ for all $i_1 \leq l \leq i_b$) is any linear combination of Arihant weight w or less of the columns from amongst any b (or fewer) consecutive blocks of columns out of the previously chosen $(j-1)$ blocks.

The number of ways in which the coefficients λ_i can be chosen is given by

$$\sum_{\lambda=1}^{[q/2]}((Q_\lambda)^{n_j}-(Q_{\lambda-1})^{n_j})V_{t-1-\lambda,q}^{(n_1,n_2,\cdots,n_{j-1})}, \tag{14}$$

where

$$1 \leq \lambda = w_A(\lambda_j) \leq [q/2].$$

Since all possible linear combinations of Arihant weight $(t-1)$ or less are included in (14), therefore, the coefficients α_i $(j-b+1 \leq i \leq j)$ and β_l $(i_1 \leq l \leq l_b)$ should be chosen so that the sum of their Arihant weights is at least t.

To obtain the number of all possible distinct linear combinations, we analyze three different cases:

Case 1. When the blocks H_l $(i_1 \leq l \leq i_b)$ are taken from the first $(j-b)$ blocks.

In this case, choose $\alpha_i (1 \leq i \leq j)$ such that the sum of their Arihant weights is equal to a number p_1 and β_l $(i_i \leq l \leq i_b)$ having sum of their Arihant weights equal to p_2 such that $p_1+p_2 \geq t$. The largest value which p_1 and p_2 can attain is w.

Now α_i $(1 \leq i \leq j)$ with sum of their Arihant weights equal to p_1 can be chosen in

$$\sum_{\lambda=1}^{[q/2]}((Q_\lambda)^{n_j}-(Q_{\lambda-1})^{n_j})A_{p_1-\lambda,q}^{(n_{j-b+1},\cdots,n_{j-1})} \tag{15}$$

To choose β_l $(i_1 \leq l \leq i_b)$ with sum of their Arihant weights equal to p_2 is equivalent to evaluating the number of P-bursts of block length b or less with Arihant weight p_2 in a blcok vector of length $n_1+n_2+\cdots+n_{j-b}$. This can be done (by Lemma 4.2) in

$$C_q\left(b, \sum_{i=1}^{j-b} n_i, p_2\right) \text{ ways.} \tag{16}$$

Case 2. When the blocks H_l $(i_1 \leq l \leq i_b)$ are taken from the immediately prceding $(b-1)$ blocks.

The additonal number of ways in which the coefficients α_i $(j-b+1 \leq i \leq j)$ and β_i $(i_1 \leq l \leq i_b)$ can be chosen are given by

$$\sum_{\lambda=1}^{[q/2]}((Q_\lambda)^{n_j}-(Q_{\lambda-1})^{n_j})C_q^*(b-1, \sum_{i=j-b+1}^{j-1} n_i, 2t-\lambda, 2w-\lambda). \tag{17}$$

Case 3. When the blocks H_l $(i_1 \leq l \leq i_b)$ are selected from H_{j-2b+2}, $H_{j-2b+3}, \cdots, H_{j-1}$ such that all are neither taken from $H_{j-2b+2}, \cdots, H_{j-b}$ nor from $H_{j-b+1}, H_{j-b+2}, \cdots, H_{j-1}$.

Let us supose that the P-burst starts from the $(j-2b+k+1)^{th}$ block position which may continue upto $(j-b+k)^{th}$ block position $(1 \leq k \leq b-1)$. Also, let the Arihant weight of the $(j-2b+k+1)^{th}$ block be θ where $1 \leq \theta \leq \min([q/2], w-1)$. The total number of choices for selecting the components of $(j-2b+k+1)^{th}$ block is given by

$$(Q_\theta)^{n_{j-2b+k+1}} - (Q_{\theta-1})^{n_{j-2b+k+1}}.$$

Our objective is to select non-zero blcoks from the $(j-2b+k+1)^{th}, (j-2b+k+2)^{th}, \cdots, (j-b)^{th}, (j-b+1)^{th}, \cdots, (j-b+k)^{th}, (j-b+k+1)^{th}, \cdots, (j-b)^{th}$ blocks having sum of their Arihant weight w or less or this, let us have linear combinations of Arihant weight $r_{1\theta}$ of blocks of columns from the $(j-2b+k+2)^{th}, \cdots, (j-b)^{th}$ blocks; linear combination of Arihant weight $r_{2\theta}$ of columns from the $(j-b+1)^{th} \cdots, (j-b+k)^{th}$ blocks and lienar combinations of Arihant weight $r_{3\theta}$ of columns from the $(j-b+k+1)^{th}, \cdots, (j-)^{th}$ blocks. Then the total number of choices for the coeffcients α_i $(1 \leq i \leq j)$ and β_l $(i_1 \leq l \leq l_b)$ in Case 3 is given by

$$\begin{aligned}
&\sum_{\lambda=1}^{[q/2]} \Big((Q_\lambda)^{nj} - (Q_{\lambda-1})^{nj} \Big) \\
&\Bigg(\sum_{k=1}^{b-1} \sum_{\theta=1}^{(min[q/2], w-1)} \sum_{r_{1\theta}, r_{2\theta}, r_{3\theta}} \\
&((Q_\theta)^{n_{j-2b+k+1}} - (Q_{\theta-1})^{n_{j-2b+k+1}}) \, A_{r_{1\theta},q}^{(n_{j-2b+k+1}, \cdots, n_{j-b})} \times \\
&A_{r_{2\theta},q}^{(n_{j-b+1}, \cdots, n_{j-b+k})} A_{r_{3\theta},q}^{(n_{j-b+k+1}, \cdots, n_{j-1})} \Bigg),
\end{aligned} \tag{18}$$

where

$$\begin{aligned}
&1 \leq \theta + r_{1\theta} \leq w-1; \\
&1 \leq +r_{2\theta} \leq 2w-1-\lambda; \\
&0 \leq +r_{3\theta} \leq w-\lambda; \\
&r_{2\theta} + r_{3\theta} \geq t-\lambda; \\
&\theta + r_{1\theta} + r_{2\theta} \geq t \\
&2t-\lambda \leq \theta + r_{1\theta} + r_{2\theta} + r_{3\theta} \leq 2w-\lambda.
\end{aligned}$$

Thus the total number of linear combinations occuring in all the three cases is given by

$$(14) + \Bigg(\sum_{\substack{p_1, p_2: \\ p_1+p_2=t}}^{p_1+p_2=2w} (15) \times (16) \Bigg) + (17) + (18)$$

$$
\begin{aligned}
= & \sum_{\lambda=1}^{[q/2]}((Q_\lambda)^{n_j}-(Q_{\lambda-1})^{n_j})V_{t-1-\lambda,q}^{(n_1,n_2,\cdots,n_{j-1})}+ \\
& \Bigg(\sum_{\substack{p_1,p_2;\\ p_1+p_2=t}}^{p_1+p_2=2w[q/2]}\sum_{\lambda=1}((Q_\lambda)^{n_j}-(Q_{\lambda-1})^{n_j})A_{p_1-\lambda,q}^{(n_{j-b+1},\cdots,n_{j-1})}\times \\
& C_q(b,\sum_{i=1}^{j-b}n_i,p_2))\Bigg)+\sum_{\lambda=1}^{[q/2]}((Q_\lambda)^{n_j}-(Q_{\lambda-1})^{n_j})\times \\
& C_q^*(b-1,\sum_{i=j-b+1}^{j-1}n_i,2t-\lambda,2w-\lambda))+\sum_{\lambda=1}^{[q/2]}((Q_\lambda)^{nj}-(Q_{\lambda-1})^{nj})\times \\
& \Bigg(\sum_{k=1}^{b-1}\sum_{\theta=1}^{(min[q/2],w-1)}\sum_{r_{1\theta},r_{2\theta},r_{3\theta}} \\
& ((Q_\theta)^{n_{j-2b+k+1}}-(Q_{\theta-1})^{n_{j-2b+k+1}})\,A_{r_{1\theta},q}^{(n_{j-2b+k+1},\cdots,n_{j-b})}\times \\
& A_{r_{2\theta},q}^{(n_{j-b+1},\cdots,n_{j-b+k})}A_{r_{3\theta},q}^{(n_{j-b+k+1},\cdots,n_{j-1})}\Bigg), \\
= & \ L \quad \text{(say)}.
\end{aligned}
$$

Hence the j^{th} block H_j of block size n_j can be added to the parity check matrix H if the number of available $(n-k)$-vectors which is q^{n-k} in number is at least as large as L i.e. if

$$q^{n-k} \geq L. \tag{19}$$

For the existence of an $[n,k;P]$ LPA code where $n=n_1+n_2+\cdots+n_s$, the inequality (19) must hold for $j=s$ so that it is possible to add upto s^{th} block H_s to form an $(n-k)\times n$ block matrix H and we get (10). □

Corollary 4.5. *Taking $t=1$ in Theorem 4.4., we get a sufficient bound for weighted P-burst error correction in LPA codes analogous to classical Campopiano bound [1].*

5. Conclusion.

In this paper, we have obtained a sufficient bound which is infact a construction upper bound for LPA codes correcting weighted P-burst errors and simultaneously detecting random block errors. The bound obtained is an extended Campopiano's type bound for LPA codes.

Acknowledgment. The first author would like to thank her spouse Prof.(Dr.) Arihant Jain for his constant support and encouragement for pursuing research.

References

[1] C.N. Campopiano, *Bounds on Burst Error Correcting Codes*, IRE. Trans., IT-8 (1962), 257-259.

[2] K. Feng, L. Xu and F.J. Hickernell, *Linear Error-Block codes*, Finite Fields and Applications, 12(2006), 638-652.

[3] S. Jain, *Linear Partition Codes in Arihant Metric*, World Applied Sciences Journal, 14(12) (2011), 1900-1907.

[4] S. Jain, A.K. Mishra and K.P. Shum, *Weight distribution of LPA codes and their duals*, Algebras, Groups, Geometries, 32(2015), 369-386.

[5] S. Jain, *P-bursts in lpγ-spaces*, World Applied Sciences Journal, 30 (2014), 1977-1984.

[6] S. Jain, *On extended Hamming sphere bound in LPA codes*, Southeast Asian Bulletin of Mathematics, 40 (2016), 341-351.

[7] S. Jain, K.B. Nam and K.-S. Lee, *On Some Perfect Codes with respect to Lee Metric, Linear Algebra and Its Applications*, 405 (2005), 104-120.

[8] C.Y. Lee, *Some properties of non-binary error correcting codes*, IEEE Trans. Information Theory, IT-4 (1958), 77-82.

[9] J.H. van Lint, Introduction to Coding Theory, Third Edition, Springer Verlag, Heidelberg, Germany, 1998.

ALGEBRAS GROUPS AND GEOMETRIES 35 427 - 449 (2018)
DOI 10.29083/AGG.35.04.2018

UNIFORMLY INDEPENDENT I-SPOTTY-BYTE ERROR CONTROL CODES

Sapna Jain
Shanxi Normal University
P. R. China
sapnajain@gmx.com

Received February 7, 2020
Revised June 17, 2020

Abstract

In [5], the author has devised uniform i-spotty-byte error control codes which are suitable for semi-conductor memories where an I/O word is divided into irregular bytes not necessarily of the same length with those of equal length aligned together constituting a "sector" and uniform i-spotty-byte errors are defined as i-spotty-byte errors confined to a particular sector. The author also discussed the code design of uniform i-spotty-byte error control codes and their decoding. However, an important and practical situation is when uniform i-spotty-byte errors caused by the hit of high energetic particles are independent in nature in the sense that sum of the erroneous i-bytes is non-zero. Keeping this in view, in this paper, we propose a new model of uniform i-spotty-byte errors viz. "uniformly independent i-spotty byte errors" which are capable of correcting all uniformly independent i-spotty-byte errors of measure μ(or less). It has been further shown that these codes require fewer number of check bits than the earlier defined uniform i-spotty byte error control codes [5] and/or usual i-spotty-byte error control codes [4] meaning thereby that the rate of storage of these codes is higher than the other ones. Also, the decoding algorithm presented in this paper for uniformly independent i-spotty byte error control codes is greatly simplified than those for the uniform i-spotty byte error control codes.

Keywords: Uniform i-spotty-byte errors, i-spotty-byte distance, error control codes

Copyright © 2018 by Hadronic Press Inc., Palm Harbor, FL 34682, U.S.A.

1. Introduction

The uniform i-spotty-byte error control codes devised by the author [5] are suitable for semiconductor memories consisting of irregular RAM chips not necessarily of the same size and those of same length are aligned together and errors caused by the hit of high energetic particles are confined to adjacent i-bytes/RAM chips of the same size only. However, an important and practical situation is when uniform i-spotty-byte errors are independent in nature in the sense that sum of the erroneous i-bytes in the erroneous sector is non-zero. Keeping this in view, this paper proposes a new model of uniform i-spotty-byte error viz."uniformly independent i-spotty byte errors" and presents code for the correction of the same. It has been shown that the rate of storage of uniformly independent i-spotty byte error control codes is higher than the usual i-spotty byte error control codes and uniform i-spotty byte error codes. The paper also presents a decoding algorithm for uniformly independent i-spotty-byre error correcting code which is simplified in the sense of determining the erroneous sector in comparison to the decoding algorithm for uniform i-spotty byte error correcting codes.

2. Definitions and Notations

Let $q = p^m$ be a power of prime number p and $\mathbf{F}_q$ be the finite field with q elements. A partition, P, of a positive integer N is defined as

$$P : N = m_1 + m_2 + \cdots + m_g, 1 \leq m_1 \leq m_2 \cdots \leq m_g \quad g \geq 1.$$

and is denoted as

$$P = [m_1][m_2]\cdots[m_g] = [n_1]^{\lambda_1}[n_2]^{\lambda_2}\cdots[n_s]^{\lambda_s},$$

if

$$\begin{aligned}
&m_1 = m_2 = \cdots = m_{\lambda_1} = n_1,\\
&m_{\lambda_1+1} = m_{\lambda_1+2} = \cdots = m_{\lambda_1+\lambda_2} = n_2,\\
&\vdots\\
&\vdots\\
&\vdots\\
&m_{\lambda_1+\lambda_2+\cdots+\lambda_{s-1}+1} = m_{\lambda_1+\lambda_2\cdots\lambda_{s-1}+2}\\
&= \cdots = m_{\lambda_1+\lambda_2+\cdots+\lambda_s} = n_s.
\end{aligned}$$

Then we can write the field $\mathbf{F}_q^N$ as

$$\mathbf{F}_q^N = \mathbf{F}_q^{m_1} \oplus \mathbf{F}_q^{m_2} \oplus \cdots \oplus \mathbf{F}_q^{m_g}$$

$$= \bigoplus_{i=1}^{s}\Big(\bigoplus_{\lambda_i - copies} \mathbf{F}_q^{n_i}\Big).$$

Each vector $v \in \mathbf{F}_q^N = \bigoplus_{i=1}^{s}(\bigoplus_{\lambda_i - copies} \mathbf{F}_q^{n_i})$ can be uniquely written as $v = (v_1, v_2, \cdots, v_s)$ where $v_j \in (\mathbf{F}_q^{n_j})^{\lambda j}$ for all $1 \leq j \leq s$ and is represented as

$$v_j = (v_j^0, v_2^1, \cdots, v_j^{\lambda j-1}), \quad v_j^a \in \mathbf{F}_q^{n_j} \text{ for all } 0 \leq a \leq \lambda_{j-1}, \tag{1}$$

or equivalently

$$\begin{aligned} v_j \;=\; & (v_j^{(0,1)}, v_j^{(0,2)}, \cdots, v_j^{(0,n_j)}, v_j^{(1,1)}, v_j^{(1,2)}, \cdots, v_j^{(1,n_j)}, \cdots \\ & \cdots, v_j^{(\lambda j-1,1)}, v_j^{(\lambda j-1,2)}, \cdots, v_j^{(\lambda_j-1,n_j)}), \end{aligned}$$

where $v_j^a = (v_j^{(a,1)}, v_j^{(a,2)}, \cdots, v_j^{(a,n_j)})$, $v_j^{(a,b)} \in \mathbf{F}_q$ for all $0 \leq a \leq \lambda_j - 1$ and $1 \leq b \leq n_j$. Here $v_j (1 \leq j \leq s)$ is called the "j^{th} sector of v" consisting of λ_j i-bytes viz. $v_j^0, v_j^1, \cdots, v_j^{\lambda_j - 1}$ each of length n_j. Thus the length of the j^{th} sector v_j is $\lambda_j n_j$. The partition P is named as *primary partition* or *irregular-byte partition.* Further, let $1 \leq T \leq N$ be a positive integer such that $P' : T = [t_1]^{\lambda_1}[t_2]^{\lambda_2} \cdots [t_s]^{\lambda_s}$ be a partition of T where $1 \leq t_i \leq n_i$ for all $1 \leq i \leq s$ and also $1 \leq t_1 \leq t_2 \leq \cdots \leq t_s$. Then P' is called as the *"secondary partition"* or *"error partition"*. Note that the secondary partition depends upon the primary partition. The number N is called the *primary number* and the number T is called the *secondary number.*

Clearly,

$$N = \lambda_1 n_1 + \lambda_2 n_2 + \cdots + \lambda_s n_s$$

and

$$T = \lambda_1 t_1 + \lambda_2 t_2 + \cdots + \lambda_s t_s.$$

We give below few definitions given in [5].

Definition 2.1 [5]. Let N and T be the primary and secondary numbers respectively as discussed in the preceeding paragraph corresponding to the partitions P and P' resp. given by

$$\begin{aligned} P : N \;&=\; [n_1]^{\lambda_1}[n_2]^{\lambda_2} \cdots [n_s]^{\lambda_s}, \\ \text{and} & \\ P' : T \;&=\; [t_1]^{\lambda_1}[t_2]^{\lambda_2} \cdots [t_s]^{\lambda_s}, \end{aligned}$$

where $1 \leq t_i \leq n_i$ for all $1 \leq i \leq s$.

Let $v = (v_1, v_2, \cdots, v_s)$ be a vector in $\mathbf{F}_q^N = \bigoplus_{i=1}^{s}\Big(\bigoplus_{\lambda_i - copies} \mathbf{F}_q^{n_i} \Big)$ as given in (1). The *irregular-spotty-byte weight* (or simply *i-spotty-byte weight*) $w_\beta^{(P,P')}(v)$ corresponding to the primary partition P and secondary partition P' is given by

$$w_\beta^{(P,P')}(v) = \sum_{i=1}^{s} \sum_{a=0}^{\lambda_i - 1} \left\lceil \frac{\sum_{b=1}^{n_i} w_H(v_i^{(a,b)})}{t_i} \right\rceil, \tag{2}$$

where $\sum_{b=1}^{n_i} w_H(v_i^{(a,b)})$ is the Hamming weight of the a^{th} i-byte in the i^{th} sector v_i and $\lceil x \rceil$ denotes the smallest integer greater than or equal to x.

Definition 2.2 [5]. The *irregular-spotty distance* (or simply *i-spotty distance*) between two vectors $u, v \in \mathbf{F}_q^N$ corresponding to the primary partition P and secondary partition P' is given by

$$\begin{aligned} d_\beta^{(P,P')}(u,v) = w_\beta^{(P,P')}(u-v) &= \sum_{i=1}^{s} \sum_{a=0}^{\lambda_i - 1} \left\lceil \frac{\sum_{b=1}^{n_i} w_H(u_i^{(a,b)} - v_i^{(a,b)})}{t_i} \right\rceil \\ &= \sum_{i=1}^{s} \sum_{a=0}^{\lambda_i - 1} \left\lceil \frac{\sum_{b=1}^{n_i} d_H(u_i^{(a,b)}, v_i^{(a,b)})}{t_i} \right\rceil, \end{aligned} \tag{3}$$

where $\sum_{b=1}^{n_i} d_H(u_i^{(a,b)}, v_i^{(a,b)})$ is the Hamming distance between the a^{th} i-bytes of the i^{th} sectors u_i and v_i of u and v respectively. Then i-spotty-byte distance is a metric function.

Note. We also call the i-spotty weight and i-spotty distance as "t_i/n_i-weight" and "t_i/n_i-distance" respectively. Moreover, we simply denote the i-spotty weight $w_\beta^{(P,P')}$ and i-spotty distance $d_\beta^{(P,P')}$ by w_β and d_β respectively when the primary partition P and secondary partition P' are clear from the context.

Definition 2.3 [5]. Let T and N be the primary and secondary numbers corresponding to the primary and secondary partitions P and P' resp. where P and P' are given by

$$P : N = [n_1]^{\lambda_1}[n_2]^{\lambda_2} \cdots [n_s]^{\lambda_s},$$

$$P' : T = [t_1]^{\lambda_1}[t_2]^{\lambda_2}\cdots[t_s]^{\lambda_s},$$

and $1 \leq t_i \leq n_i$ for all $1 \leq i \leq s$.

Let $V \subseteq \mathbf{F}_q^N = \bigoplus_{i=1}^{s}\Big(\bigoplus_{\lambda_i - copies} \mathbf{F}_q^{n_i}\Big)$ be an $\mathbf{F}_q$ subspace of $\mathbf{F}_q^N$ equipped with the i-spotty-byte metric d_β. Then V is called an *"irregular-spotty-byte"* (or simply *"i-spotty-byte"*) error control code and is denoted by $[N, k, d_\beta; P, P']$ where

$$\begin{aligned} N &= n_1\lambda_1 + n_2\lambda_2 + \cdots + n_s\lambda_s \\ &= \text{length of the code,} \\ k &= \dim_{\mathbf{F}_q}(V), \text{ and} \\ d_\beta &= \min_{\substack{x,y\in V \\ x\neq y}} d_\beta(x, y). \end{aligned}$$

3. Uniformly independent i-spotty-byte error control codes

In this section, we define uniformly independent i-spotty-byte errors and then design codes to control these types of errors. We begin with the definition of vectors of i-spotty weight or i-spotty measure $\mu(\mu \geq 1)$ in relation to Definition 2.1.

Definition 3.1. Let $v = (v_1, v_2, \cdots, v_s) \in \mathbf{F}_q^N = \bigoplus_{i=1}^{s}(\bigoplus_{\lambda_i - copies} \mathbf{F}_q^{n_i})$. If $w_\beta(v) = w_\beta^{(P,P')}(v) = \mu$, where $w_\beta^{(P,P')}(v)$ is given by (2), then we say that *i-spotty-weight* or *i-spotty measure of v is $\mu(\mu \geq 1)$* or equivalently we say that *t_i/n_i-measure of v is μ*.

Definition 3.2. A *"uniformly independent i-spotty-byte error"* of i-spotty measure μ is an error vector of i-spotty measure μ in which all the erroneous digits are confined to i-bytes of the same sector and the sum of erroneous i-bytes is non-zero.

Note. Every uniformly independent i-spotty-byte error is a uniform i-spotty-byte error but not conversely.

Example 3.3. Let $q = 2, N = 13, T = 9$ and

$$\begin{aligned} P &: N = 13 = [1]^3[2]^2[3]^2, \\ P' &: T = 9 = [1]^3[1]^2[2]^2, \end{aligned}$$

be the primary and secondary partitions corresponding to $N = 13$ and $T = 9$ respectively. Then $u = (0\ \ 0\ \ 0\ \vdots\ 00\ \ 00\ \vdots\ 110\ \ 011) \in \mathbf{F}_2^{13}$ is a uniformly independent i-spotty-byte error of measure 2. But $v = (0\ \ 0\ \ 0\ \vdots\ 00\ \ 00\ \vdots\ 110\ \ 110) \in \mathbf{F}_2^{13}$ is not a uniformly

independent i-spotty-byte error of measure 2 but it is a uniform i-spotty-byte error of measure 2.

We now define $r \times r$ companion matrix over $\mathbf{F}_q$ [1,6]:

Definition 3.4 [1,6]. Given a monic primitive polynomial $g(x)$ of degree r over $\mathbf{F}_q$, the $r \times r$ companion matrix M corresponding to $g(x)$ is defined as follows:

$$g(x) = g_0 + g_1 x + g_2 x^2 + \cdots\cdots + g_{r-2} x^{r-2} + g_{r-1} x^{r-1} + x^r,$$

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & -g_0 \\ 1 & 0 & \cdots & 0 & 0 & -g_1 \\ 0 & 1 & \cdots & 0 & 0 & -g_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & -g_{r-2} \\ 0 & 0 & \cdots & 0 & 1 & -g_{r-1} \end{pmatrix}_{r \times r}$$

Observations.

(i) Let α be a primitive element of $\mathbf{F}_q^r$ and a root of $g(x)$. Its companion matrix M has its columns $\begin{pmatrix} \vdots \\ \alpha^i \\ \vdots \end{pmatrix}$ for $i = 1$ to r where $\begin{pmatrix} \vdots \\ \alpha^i \\ \vdots \end{pmatrix}$ is the coefficient vector of $x^i (mod\ g(x))$.

The companion matrix of α^j is M^j and its column vectors are expressed as follows:

$$M^j = \begin{pmatrix} \vdots & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots \\ \alpha^j & \alpha^{j+1} & \cdots & \alpha^{j+r-1} \\ \vdots & \vdots & \cdots & \vdots \\ \vdots & \vdots & \cdots & \vdots \end{pmatrix}_{r \times r}.$$

Let e be the exponent of $g(x)$, that is, $y = e$ is the least positive solution of $x^y \equiv (mod\ g(x))$. The companion matrix M has the following properties [1,6]:

(a) M is non singular.

(b) $M^0 = M^e = I_r$.

(c) $M^i = M^j$ if and only if $i \equiv j(mod\ e)$.

Now, we present the code construction method of uniformly independent i-spotty-byte error control codes using the following definition:

Definition 3.5. Let q be a prime number or power of a prime number. Let $\mu, n_1 \leq n_2 \leq \cdots \leq n_s$ and $t_1 \leq t_2 \leq \cdots \leq t_s$ be positive integers with $1 \leq t_i \leq n_i$ for all $1 \leq i \leq s$. Define

$$t = \max_{j=1}^{s}\{t_j\} \quad \text{and} \quad n = \max_{j=1}^{s}\{n_j\}.$$

Further, for each $j = 1$ to s, let

(i) $m_j = q^{n_j} - 1$;

(ii) I_{n_j} be the $n_j \times n_j$ identity matrix and $O_{n_i} \times n_j$ be the $n_i \times n_j$ null matrix over $\mathbf{F}_q$ for all $1 \leq i \leq s$;

(iii) M_j' be the $n_j \times n_j$ companion matrix corresponding to a q-ary primitive polynomial $g_j(x)$ of degree n_j;

(iv) $(M_j)^{i_j}$ be the $n \times n_j$ extended matrix obtained from the $n_j \times n_j$ matrix $(M_j')^{i_j}$ by adding $(n - n_j)$ all-zero rows to it for all $0 \leq i_j \leq m_j - 1$. We call M_j as the *extended companion matrix with respect to* M_j'.

Theorem 3.6. *Using the notations as given in Definitions 3.5, the null space of matrix* H *where*

$$H = \begin{pmatrix} H_1' & H_2' & \cdots & H_s' \\ H_1'' & H_2'' & \cdots & H_s'' \end{pmatrix},$$

and each $H_j'(1 \leq j \leq s)$ *is a* $(\sum_{j=1}^{s} n_j) \times (m_j n_j)$ *submatrix and each* $H_j''(1 \leq j \leq s)$ *is a*

$((2\mu-1)n)\times(m_jn_j)$ *submatrix given by*

$$H'_j = \begin{pmatrix} O_{n_1\times n_j} & O_{n_1\times n_j} & \cdots & O_{n_1\times n_j} \\ O_{n_2\times n_j} & O_{n_2\times n_j} & \cdots & O_{n_2\times n_j} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ O_{n_{j-1}\times n_j} & O_{n_{j-1}\times n_j} & \cdots & O_{n_{j-1}\times n_j} \\ I_{n_j} & I_{n_j} & \cdots & I_{n_j} \\ O_{n_{j+1}\times n_j} & O_{n_{j+1}\times n_j} & \cdots & O_{n_{j+1}\times n_j} \\ \vdots & \vdots & \vdots & \\ \vdots & \vdots & \vdots & \\ O_{n_s\times n_j} & O_{n_s\times n_j} & \cdots & O_{n_s\times n_j} \end{pmatrix}_{(\sum_{j=1}^{s} n_j)\times(m_jn_j)},$$

$$H''_j = \begin{pmatrix} M_j^0 & M_j^1 & \cdots & (M_j)^{(m_j-1)} \\ M_j^0 & M_j^2 & \cdots & (M_j)^{2(m_j-1)} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ M_j^0 & (M_j)^{(2\mu-1)} & \cdots & (M_j)^{(2\mu-1)(m_j-1)} \end{pmatrix}_{(2\mu-1)n\times(m_jn_j)}.$$

is a uniformly independent i-spotty-byte error control code correcting all uniformly independent i-spotty-byte errors of measure μ or less and having check bit length $R = \sum_{j=1}^{s} n_j + (2\mu-1)n$ and code length $N = m_1n_1 + m_2n_2 + \cdots + m_sn_s$. The parameters of the resulting code will be

$$[N, N-R, d; P, P'],$$

where $P : N = [n_1]^{m_1}[n_2]^{m_2}\cdots[n_s]^{m_s}$, $P' : T = [t_1]^{m_1}[t_2]^{m_2}\cdots\cdots[t_s]^{m_s}$ and $d \le 2\mu+1$.

Proof. It suffices to prove that the code V which is the null space of H detects all i-spotty-byte errors of measure 2μ or less with errors occuring in the same sector and sum of erroneous i-bytes be non-zero meaning thereby that the code corrects all uniformly independent i-spotty-byte errors of measure μ or less.

Let $e \in \mathbf{F}_q^N = \bigoplus_{j=1}^{s}\Big(\bigoplus_{m_j-copies}\mathbf{F}_q^{n_j}\Big)$.

Then e is of the form

$$e = (e_1, \cdots, e_s)$$

$$= \quad (e_1^0, e_1^1, \cdots, e_1^{m_1-1}, e_2^0, e_2^1, \cdots, e_2^{m_2-1}, \cdots, e_s^0, e_s^1, \cdots, e_s^{m_s-1}),$$

where $e_j^{u_j} \in \mathbf{F}_q^{n_j}$ for all $1 \leq j \leq s$ and $0 \leq u_j \leq m_j - 1$.

Suppose $w_\beta(e) \leq 2\mu$ with erroneous i-bytes confined to a single sector and sum of erroneous i-bytes is non-zero. Let j^{th} sector e_j be the erroneous sector having erroneous i-bytes say $e_j^{u_1}, e_j^{u_2}, \cdots, e_j^{u_{j^*}}$ with

$$\sum_{k=1}^{j^*} \left\lceil \frac{w_H(e_j^{u_k})}{t_j} \right\rceil \leq 2\mu,$$

and $e_j^{u_1} + e_j^{u_2} + \cdots + e_j^{u_{j^*}} \neq 0$.

Then $eH^T = 0$ gives the following relation:

$$\begin{aligned}
& [e_j^{u_1}(I_{n_j})^T \quad e_j^{u_1}(M_j^{u_1})^T \quad e_j^{u_1}(M_j^{2u_1})^T \cdots\cdots e_j^{u_1}(M^{(2\mu-1)u_1})^T] \\
& +[e_j^{u_2}(I_{n_j})^T \quad e_j^{u_2}(M_j^{u_2})^T \quad e_j^{u_2}(M_j^{2u_2})^T \cdots\cdots e_j^{u_2}(M^{(2\mu-1)u_2})^T] \\
& +\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
& +\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
& +[e_j^{u_{j^*}}(I_{n_j})^T \quad e_j^{u_{j^*}}(M^{u_{j^*}})^T \quad e_j^{u_{j^*}}(M^{2u_{j^*}})^T \cdots\cdots e_j^{u_{j^*}}(M^{(2\mu-1)u_{j_*}})^T] \\
= \quad & [O_{n_j} \quad O_n \quad O_n \cdots\cdots O_n],
\end{aligned}$$

where O_{n_j} and O_n are the $1 \times n_j$ and $1 \times n$ null matrices respectively.

Writing the above equation in the matrix form gives

$$\begin{aligned}
& (e_j^{u_1}, e_j^{u_2}, \cdots, e_j^{u_{j^*}}) \times \\
& \times \begin{pmatrix}
I_{n_j} & (M_j^{u_1})^T & (M_j^{2u_1})^T & \cdots & (M_j^{(2\mu-1)u_1})^T \\
I_{n_j} & (M_j^{u_2})^T & (M_j^{2u_2})^T & \cdots & (M_j^{(2\mu-1)u_2})^T \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
I_{n_j} & (M_j^{u_{j^*}})^T & (M^{(2u_{j^*})})^T & \cdots & (M_j^{(2\mu-1)u_{j^*}})^T
\end{pmatrix} \\
& = (O_{n_j}, O_n, O_n, \cdots, O_n).
\end{aligned}$$

Replacing the extended companion matrix M_j by the corresponding companion matrix M_j' in the above matrix equation results in an equivalent matrix equation and is given

by

$$(e_j^{u_1}, e_j^{u_2}, \cdots, e_j^{u_{j^*}}) \times$$

$$\times \begin{pmatrix} I_{n_j} & (M_j')^{u_1})^T & ((M_j')^{2u_1})^T & \cdots & ((M_j')^{(2\mu-1)u_1})^T \\ I_{n_j} & (M_j')^{u_2})^T & ((M_j')^{2u_2})^T & \cdots & ((M_j')^{(2\mu-1)u_2})^T \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ I_{n_j} & (M_j')^{u_{j^*}})^T & ((M_j')^{(2u_{j^*})})^T & \cdots & ((M_j')^{(2\mu-1)u_{j^*}})^T \end{pmatrix}$$

$$= (O_{n_j}, O_{n_j}, O_{n_j}, \cdots, O_{n_j}),$$

or equivalently

$$(e_j^{u_1}, e_j^{u_2}, \cdots, e_j^{u_{j^*}}) \times$$

$$\times \begin{pmatrix} I_{n_j} & I_{n_j} & \cdots & I_{n_j} \\ (M_j')^{u_1} & (M_j')^{u_2} & \cdots & (M_j')^{u_{j^*}} \\ \vdots & \vdots & \vdots & \vdots \\ (M_j')^{(2\mu-1)u_1} & (M_j')^{(2\mu-1)u_2} & \cdots & (M_j')^{(2\mu-1)u_{j^*}} \end{pmatrix}^T$$

$$= (O_{n_j}, O_{n_j}, O_{n_j}, \cdots, O_{n_j}).$$

Since the total numbers j^* of erroneous i-bytes is less than or equal to 2μ, therfore, writing the above matrix equation for the top j^* relations, we get

$$(e_j^{u_1}, e_j^{u_2}, \cdots, e_j^{u_{j^*}}) \times$$

$$\times \begin{pmatrix} I_{n_j} & I_{n_j} & \cdots & I_{n_j} \\ (M_j')^{u_1} & (M_j')^{u_2} & \cdots & (M_j')^{u_{j^*}} \\ \vdots & \vdots & \vdots & \vdots \\ (M_j')^{(j^*-1)u_1} & (M_j')^{(j^*-1)u_2} & \cdots & (M_j')^{(j^*-1)u_{j^*}} \end{pmatrix}^T$$

$$= (O_{n_j}, O_{n_j}, \cdots, O_{n_j}).$$

The coefficient matrix being Vandermonde's matrix is non-singular. Therefore, the above system of equations have a solution viz.

$$e_j^{u_1} = e_j^{u_2} = \cdots = e_j^{u_{j^*}} = O_{n_j}$$

which implies that $e = 0$, A contradiction. Thus $eH^T \neq 0$ and hence H is the null space of an i-spotty-byte code correcting all uniformly independent i-spotty-byte errors of measure μ or less. □

Note. We may also have a shortened version of the code discussed in Theorem 3.6 by choosing integers $\lambda_1, \lambda_2, \cdots, \lambda_s$ such that $1 \leq \lambda_j \leq m_j$ for all $j = 1$ to s and then keeping only first $\lambda_j n_j$ columns of he submatrices H_j' and H_j''. The parameters of the shortened code will be $[N, N - R, d; P, P']$ where

$$\begin{aligned} N &= \lambda_1 n_1 + \lambda_2 n_2 + \cdots + \lambda_s n_s, \\ R &= \sum_{i=1}^{s} n_i + (2\mu - 1)n, \\ P : N &= [n_1]^{\lambda_1}[n_2]^{\lambda_2} \cdots [n_s]^{\lambda_s}, \\ P' : T &= [t_1]^{\lambda_1}[t_2]^{\lambda_2} \cdots\cdots [t_s]^{\lambda_s}, \text{and} \\ d &\leq 2\mu + 1. \end{aligned}$$

4. Decoding of uniformly independent i-spotty-byte error correcting codes

In this section, we present a decoding algorithm for the uniformly independent i-spotty-byte error correcting codes.

Let V be an i-spotty-byte code correcting all uniformly independent i-spotty-byte errors of measure μ or less. Let u, r and e be the transmitted codeword, the received word and the error vector respectively. The syndrome S of the received word r is calculated as

$$S = \begin{pmatrix} S_1 \\ S_2 \\ \vdots \\ S_{2\mu} \end{pmatrix}^T = rH^T = (u + e)H^T = eH^T,$$

where $S_1 \in \mathbf{F}_q^{n_1+n_2+\cdots+n_s}$ is a $(n_1 + n_2 + \cdots + n_s)$-bit q-ary row vector and $S_i \in \mathbf{F}_q^n$ for all $2 \leq i \leq 2\mu$.

The decoding is done as follows:

Step 1.

(i) If $S_1 = S_2 = \cdots \simeq S_{2\mu} = 0$, then there is no error during the process of communication.

(ii) If $S_1 \neq 0$ and all of $S_2 = S_3 = \cdots = S_{2\mu} = 0$, then an uncorrectable error pattern of measure greater than μ has occured and a retransmission is sought.

(iii) If $S_1 = 0$ and either of $S_2, S_3, \cdots, S_{2\mu} \neq 0$, then we infer that sum of erroneous i-bytes in the erroneous sector is zero meaning thereby that the errors are not uniformly independent and again a retransmission is sought.

(iv) If $S_1 \neq 0$ and at least one of $S_2, S_3, \cdots S_{2\mu}$ is non-zero, then for the decoding purpose, the pattern of S_1 indicates the erroneous sector position as explained below:

We partition S_1 into different blocks of lengths $n_1, n_2, \cdots, n_s$ consecutively. Now, if the first n_1 bits in S_1 form a non-zero pattern and remaining $n_2+n_3+\cdots+n_s$ digits are all-zero, then the error is in the first sector. If the first n_1 bits in S_1 are all-zero and the next n_2 bits form a non-zero pattern and also the remaining $n_3 + n_4 + \cdots + n_s$ bits in S_1 are all-zero, then the error lies in the second sector and so on.

Step 2. From Step 1, we know the erroneous sector number say j^{th} sector is in error having i-bytes of length n_j. Now, from the patterns of $S_2, S_3, \cdots, S_{2\mu}$, we define a new syndrome vector S^* as follows:

$$S^* = \begin{pmatrix} S_1^* \\ S_2^* \\ \vdots \\ S_{2\mu}^* \end{pmatrix}^T,$$

where

$$\begin{aligned} S_1^* &= n_j\text{-bit non-zero pattern as given by } S_1, \\ S_2^* &= \text{first } n_j\text{-bits of } S_2, \\ S_3^* &= \text{first } n_j\text{-bits of } S_3 \\ &\vdots \quad\quad \vdots \\ &\vdots \quad\quad \vdots \\ S_{2\mu}^* &= \text{first } n_j\text{-bits of } S_{2\mu}. \end{aligned}$$

Step 3. After calculating the new syndrome vector S^* which is identical to the syndrome of an error vector in Reed-Solomon code with minimum distance $(2\mu+1)$ over $\mathbf{F}_q^{n_j}$, the error pattern and error location over $\mathbf{F}_q^{n_j}$ are determined by using the Berlekamp-Massey algorithm for RS codes over $\mathbf{F}_q^{n_j}$.

We illustrate the code construction method and decoding algorithm with the help of following examples:

Example 4.1. Let $q=2$, $n_1=2, n_2=3, t_1=2, t_2=2$ and $\mu=2$. Then

$$m_1 = 2^{n_1}-1 = 2^2-1 = 3, \text{ and } m_2 = 2^{n_2}-1 = 2^3-1 = 7,$$
$$t = \max_{j=1}^{2}\{t_j\} = \max\{2,2\} = 2,$$
$$n = \max_{j=1}^{2}\{n_j\} = \max\{2,3\} = 3.$$

The parameters of the code to be constructed as discussed in Theorem 3.6 are given by $R = \sum_{j=1}^{2} n_j + (2\mu-1)n = 14$ and $N = \sum_{j=1}^{2} m_j n_j = 27$.

Let M_1' be the 2×2 binary companion matrix defined by the binary primitive polynomial $g_1(x) = x^2+x+1$. Then M_1' is given by

$$M_1' = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}_{2\times 2}.$$

The 3×2 extended companion matrix M_1' is obtained by adding a row of all-zeros to M_1' and is given by

$$M_1' = \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}_{3\times 2}.$$

The various powers of extended companion matrix M_1 are given below:

$$M_1^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}_{3\times 2}, M_1^1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}_{3\times 2},$$
$$M_1^2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}_{3\times 2}, M_1^3 = M_1^0.$$

Let M_2' be the 3×3 binary companion matrix defined by the binary primitive polynomial $g_2(x) = x^3+x+1$ and is given by

$$M_2' = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}_{3\times 3}.$$

Since here $n = n_2 = 3$, therefore, the extended companion matrix M_2 is same as the companion matrix M_2' i.e. $M_2 = M_2'$. The various powers of extended companion matrix M_2 are given below

$$M_2^0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}_{3\times3}, M_2^1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}_{3\times3}, M_2^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}_{3\times3},$$

$$M_2^3 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}_{3\times3}, M_2^4 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}_{3\times3}, M_2^5 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}_{3\times3},$$

$$M_2^6 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}_{3\times3}, M_2^7 = I_3.$$

The parity check matrix of an i-spotty-byte code correcting all uniformally independent errors of measure 2 or less is given by

$$H = \begin{pmatrix} I_2 & I_2 & I_2 & \vdots & O_{2\times3} & O_{2\times3} & O_{2\times3} & O_{2\times3} & O_{2\times3} & O_{2\times3} & O_{2\times3} \\ O_{3\times2} & O_{3\times2} & O_{3\times2} & \vdots & I_3 & I_3 & I_3 & I_3 & I_3 & I_3 & I_3 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ M_1^0 & M_1^1 & M_1^2 & \vdots & M_2^0 & M_2^1 & M_2^2 & M_2^3 & M_2^4 & M_2^5 & M_2^6 \\ M_1^0 & M_1^2 & M_1^4 & \vdots & M_2^0 & M_2^2 & M_2^4 & M_2^6 & M_2^8 & M_2^{10} & M_2^{12} \\ M_1^0 & M_1^3 & M_1^6 & \vdots & M_2^0 & M_2^3 & M_2^6 & M_2^9 & M_2^{12} & M_2^{15} & M_2^{18} \end{pmatrix}_{14\times27},$$

$$= \left(\begin{array}{ccc:cccccccc}
10 & 10 & 10 & 000 & 000 & 000 & 000 & 000 & 000 & 000 \\
01 & 01 & 01 & 000 & 000 & 000 & 000 & 000 & 000 & 000 \\
00 & 00 & 00 & 100 & 100 & 100 & 100 & 100 & 100 & 100 \\
00 & 00 & 00 & 010 & 010 & 010 & 010 & 010 & 010 & 010 \\
00 & 00 & 00 & 001 & 001 & 001 & 001 & 001 & 001 & 001 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
10 & 01 & 11 & 100 & 001 & 010 & 101 & 011 & 111 & 110 \\
01 & 11 & 10 & 010 & 101 & 011 & 111 & 110 & 100 & 001 \\
00 & 00 & 00 & 001 & 010 & 101 & 011 & 111 & 110 & 100 \\
10 & 11 & 01 & 100 & 010 & 011 & 110 & 001 & 101 & 111 \\
01 & 10 & 11 & 010 & 011 & 110 & 001 & 101 & 111 & 100 \\
00 & 00 & 00 & 001 & 101 & 111 & 100 & 010 & 011 & 110 \\
10 & 10 & 10 & 100 & 101 & 110 & 010 & 111 & 001 & 011 \\
01 & 01 & 01 & 010 & 111 & 001 & 011 & 100 & 101 & 110 \\
00 & 00 & 00 & 001 & 011 & 100 & 101 & 110 & 010 & 111
\end{array}\right)_{14\times 27},$$

Let $e = (00\ \ 00\ \ 00 \vdots 100\ 010\ 000\ 000\ 000\ 000\ 000)$ be the error vector that has occured during the process of communication.

We compute the syndrome vector S as

$$S = eH^T = (S_1, S_2, S_3, S_4) = (00110, 101, 010, 111).$$

We partition S_1 into $n_1 + n_2 = 2 + 3$ bits i.e. $S_1 = (00 \quad 110)$.

Since the first n_1-bits (i.e 2 bits) of S_1 are all-zero and the remaining n_2-bits (i.e. 3 bits) are non-zero, therefore, we infer that the error lies in the second sector.

We form a new syndrome vector S^*as

$$S^* = (S_1^*, S_2^*, S_3^*, S_4^*),$$

where

$$\begin{aligned}
S_1^* &= n_2\text{-bit i.e. 3 bit non-zero pattern in } S_1 = 110, \\
S_2^* &= \text{first } n_2\text{-bits i.e. first 3 bits of } S_2 = 101, \\
S_3^* &= \text{first 3-bits of } S_3 = 010, \\
S_4^* &= \text{first 3-bits of } S_4 = 111.
\end{aligned}$$

Thus

$$S^* = (S_1^*, S_2^*, S_3^*, S_4^*) = (110, 101, 010, 111) = (\alpha^3, \alpha^6, \alpha, \alpha^5),$$

where α is a primitive element of F_2^3 defined by the polynomial $x^3 + x + 1$.

The error locator polynomial σ^* for the syndrome S^* using the Berlekamp-Massey algorithm is computed as

$$\sigma^*(x) = 1 + \alpha^3 x + \alpha x^2.$$

The degree of the error locator polynomial denotes the number of erroneous i-bytes. Thus, in this case, there are two erroneous i-bytes. The inverse of the roots of the error locator polynomial gives the positions of the erroneous i-bytes. Since the roots of $\sigma^*(x)$ are α^6 and $\alpha^0 = 1$, therefore, the inverse of the roots of $\sigma^*(x)$ are $\alpha^{-6} = \alpha^1$ and $\alpha^0 = 1$. Thus we deduce that zeroth and first i-bytes are the erroneous i-bytes in the erroneous second sector. To find the erroneous i-byte patterns, we compute the evaluator polynomial evaluator $Z^*(x)$ as given below:

$$\begin{aligned} Z^*(x) &= \sigma^*(x)S^*(x) \\ &= (1 + \alpha^3 x + \alpha x^2)(1 + S_1^* x + S_2^* x^2 + S_3^* x^3 + S_4^* x^4) \\ &= (1 + \alpha^3 x + \alpha x^2)(1 + \alpha^3 x + \alpha^6 x^2 + \alpha x^3 + \alpha^5 x^4) \\ &= 1 + \alpha x^2 \text{ (keeping the terms of degree less than or equal to 2 since there are two erroneous i-bytes).} \end{aligned}$$

Now, the erroneous i-byte patterns are given by the formula

$$e_j^i = \beta_i \left(\frac{Z^*(\beta_i^{-1})}{\prod_{k \neq i}(1 + \beta_k \beta_i^{-1})} \right),$$

where j is the erroneous sector number and $\beta_i = \alpha^i$= inverse of root of $\sigma^*(x)$ and i varies over powers occuring in α^i and gives the position of erroneous i-byte.

Here $j = 2, i = 0, 1$, $\beta_0 = \alpha^0$ and $\beta_1 = \alpha^1$.

The erroneous i-bytes e_2^0 and e_2^1 are computed as

$$\begin{aligned} e_2^0 &= \beta_0 \left(\frac{Z^*(\beta_0^{-1})}{(1 + \beta_1 \beta_0^{-1})} \right) \\ &= 1 \left(\frac{1 + \alpha.1^2}{(1 + \alpha)} \right) \\ &= 1 \left(\frac{1 + \alpha}{1 + \alpha} \right) = 1 = (100), \end{aligned}$$

$$\begin{aligned} e_2^1 &= \beta_1 \left(\frac{Z^*(\beta_1^{-1})}{(1+\beta_0\beta_1^{-1})} \right) \\ &= \alpha \left(\frac{1+\alpha(\alpha^{-1})^2}{(1+\alpha^{-1}.1)} \right) \\ &= \alpha \left(\frac{1+\alpha^{-1}}{1+\alpha^{-1}} \right) = \alpha = (010). \end{aligned}$$

Hence the error pattern is given by

$$e = (00 \;\; 00 \;\; 00 \;\vdots\; 100 \;\; 010 \;\; 000 \;\; 000 \;\; 000 \;\; 000 \;\; 000).$$

Example 4.2. Using the parameters of Example 4.1, we consider the case of double uniformly independent i-spotty-byte errors occuring in the same i-byte of the erroneous sector. For this, let the error vector be

$$e = (00 \;\; 00 \;\; 00 \;\vdots\; 000 \;\; 000 \;\; 111 \;\; 000 \;\; 000 \;\; 000 \;\; 000).$$

The syndrome vector is computed as

$$S = eH^T = (S_1, S_2, S_3, S_4) = (00111, 100, 001, 011).$$

Since the first $n_1(= 2)$ bits of S_1 are all-zero and remaining $n_2(= 3)$bits form a non-zero pattern, therefore, the error lies in the second sector.

Define

$$S^* = (S_1^*, S_2^*, S_3^*, S_4^*) = (111, 100, 001, 011) = (\alpha^5, 1, \alpha^2, \alpha^4),$$

where α is a root of $x^3 + x + 1 \in \mathbf{F}_2[x]$.

The error locator polynomial $\sigma^*(x)$ for the syndrome S^* using the Berlekamp Massey algorithm is given by

$$\sigma^*(x) = 1 + \alpha^2 x.$$

Since degree $(\sigma^*(x)) = 1$, therefore, the number of erroneous i-bytes in the erroneous second sector is 1. Also, α^5 is a root of $\sigma^*(x)$ meaning thereby that $\alpha^{-5} = \alpha^2$ gives the location of the erroneous i-byte i.e. error lies in the second i-byte of the second sector.

The evaluator polynomial $Z^*(x)$ is computed as

$$\begin{aligned} Z^*(x) &= \sigma^*(x)(x)S^*(x) \\ &= (1+\alpha^2 x)(1+\alpha^5 x + x^2 + \alpha^2 x^3 + \alpha^4 x^4) \\ &= 1 + \alpha^3 x \text{ (kleeping the terms of degree less than or} \\ &\qquad \text{equal to 1 as there is a single erroneous i-byte).} \end{aligned}$$

Now, the erroneous i-byte pattern is given by

$$e_2^2 = \alpha^2 \left(\frac{1 + \alpha^3(\alpha^{-2})}{1} \right) = \alpha^2(1+\alpha) = \alpha^2\alpha^3 = \alpha^5 = (111).$$

Hence the error pattern is given by

$$e = (00 \;\; 00 \;\; 00 \;\vdots\; 000 \;\; 000 \;\; 111 \;\; 000 \;\; 000 \;\; 000 \;\; 000).$$

Example 4.3. Let $q = 2$, $n_1 = 2, n_2 = 4, t_1 = 2, t_2 = 4$ and $\mu = 1$. Then

$$m_1 = 2^{n_1} - 1 = 2^2 - 1 = 3, \quad m_2 = 2^{n_2} - 1 = 2^4 - 1 = 15,$$
$$t = \max_{j=1}^{2}\{t_j\} = \max\{2, 4\} = 4, \quad \text{and}$$
$$n = \max_{j=1}^{2}\{n_j\} = \max\{2, 4\} = 4.$$

The parameters of the code to be constructed are given by $R = (n_1 + n_2) + (2\mu + 1)n = (2 + 4) + 4 = 10$ and $N = m_1 n_1 + m_2 n_2 = 3 \times 2 + 15 \times 4 = 66$.

Let M_1' be the 2×2 binary companion matrix defined by the binary primitive polynomial $g_1(x) = x^2 + x + 1$ as given in Example 4.1. The 4×2 extended companion matrix M_1 is obtained by adding two all-zero rows to M_1' and is given by

$$M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}_{4\times 2}.$$

The various powers of extended companion matrix M_1 are given below:

$$M_1^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}_{4\times 2}, M_1^1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}_{4\times 2}, M_1^2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}_{4\times 2}, M_1^3 = M_1^0.$$

Let M_2' be the 4×4 binary companion matrix defined by the primitive polynomial $g_2(x) = x^4 + x + 1$ and is given by

$$M_2' = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}_{4\times 4}.$$

Since here $n = n_2 = 4$, therefore, the extended companion matrix M_2 is same as the companion matrix M_2' i.e. $M_2 = M_2'$. The various powers of extended companion matrix

M_2 are given below

$$M_2^0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}_{4\times4}, M_2^1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}_{4\times4}, M_2^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}_{4\times4},$$

$$M_2^3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}_{4\times4}, M_2^4 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}_{4\times4}, M_2^5 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}_{4\times4},$$

$$M_2^6 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}_{4\times4}, M_2^7 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}_{4\times4} M_2^8 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}_{4\times4}$$

$$M_2^9 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}_{4\times4}, M_2^{10} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}_{4\times4} M_2^{11} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}_{4\times4}$$

$$M_2^{12} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}_{4\times4}, M_2^{13} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}_{4\times4} M_2^{14} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}_{4\times4},$$

$$M_2^{15} = I_4.$$

The parity check matrix H of an i-spotty-byte code correcting all uniformally independent errors of measure 1 or less is given by

$$H = (A \vdots B)_{10\times66},$$

where

$$A = \begin{pmatrix} \begin{matrix} I_2 \\ O_{4\times2} \\ \cdots \\ M_1^0 \end{matrix} & \begin{matrix} I_2 \\ O_{4\times2} \\ \cdots \\ M_1^1 \end{matrix} & \begin{matrix} I_2 \\ O_{4\times2} \\ \cdots \\ M_1^2 \end{matrix} \end{pmatrix}_{10\times6},$$

$$= \begin{pmatrix} 10 & 10 & 10 \\ 01 & 01 & 01 \\ 00 & 00 & 00 \\ 00 & 00 & 00 \\ 00 & 00 & 00 \\ 00 & 00 & 00 \\ \cdots & \cdots & \cdots \\ 10 & 01 & 11 \\ 01 & 11 & 10 \\ 00 & 00 & 00 \\ 00 & 00 & 00 \end{pmatrix}_{10\times6},$$

$$B = \begin{pmatrix} \begin{matrix} O_{2\times4} \\ I_4 \\ \cdots \\ M_2^0 \end{matrix} & \begin{matrix} O_{2\times4} \\ I_4 \\ \cdots \\ M_2^1 \end{matrix} & \begin{matrix} O_{2\times4} \\ I_4 \\ \cdots \\ M_2^2 \end{matrix} & \begin{matrix} O_{2\times4} \\ I_4 \\ \cdots \\ M_2^3 \end{matrix} & \begin{matrix} O_{2\times4} \\ I_4 \\ \cdots \\ M_2^4 \end{matrix} & \begin{matrix} O_{2\times4} \\ I_4 \\ \cdots \\ M_2^5 \end{matrix} & \begin{matrix} O_{2\times4} \\ I_4 \\ \cdots \\ M_2^6 \end{matrix} & \begin{matrix} O_{2\times4} \\ I_4 \\ \cdots \\ M_2^7 \end{matrix} & \begin{matrix} O_{2\times4} \\ I_4 \\ \cdots \\ M_2^7 \end{matrix} & \begin{matrix} O_{2\times4} \\ I_4 \\ \cdots \\ M_2^9 \end{matrix} \end{pmatrix}_{10\times60},$$

$$= \begin{pmatrix}
0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 & 0000 \\
1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 & 1000 \\
0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 & 0100 \\
0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 & 0010 \\
0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 & 0001 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
1000 & 0001 & 0010 & 0100 & 1001 & 0011 & 0110 & 1101 & 1010 & 0101 & 1011 & 0111 & 1111 & 1110 & 1100 \\
0100 & 1001 & 0011 & 0110 & 1101 & 1010 & 0101 & 1011 & 0111 & 1111 & 1110 & 1100 & 1000 & 0001 & 0010 \\
0010 & 0100 & 1001 & 0011 & 0011 & 0110 & 1101 & 0101 & 1011 & 0111 & 1111 & 1110 & 1100 & 1000 & 0001 \\
0001 & 0010 & 0100 & 1001 & 0011 & 0110 & 1101 & 1010 & 0101 & 1011 & 0111 & 1111 & 1110 & 1100 & 1000
\end{pmatrix}_{10\times 60}.$$

Let $e = (00 \;\; 00 \;\; 00 \;\vdots\; 0100\ 1000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000)$ be the error vector. Then the syndrome of the error vector e is given by

$$S = eH^T = (S_1, S_2) = (001100, 0000).$$

Since $S_1 \neq 0$ and $S_2 = 0$, thus an uncorrectable error pattern has occured and retransmission is sought. This is evident from the fact that the code which is the null space of H can correct only single i-byte errors whereas the error vector e contains double i-byte errors and hence the errors are only detected but not corrected by the decoder.

On the other hand, suppose e has single i-spotty-byte error occuring in the (say) second sector i.e. let

$$e = (0\ 0\ 00 \vdots 1100 \;\; 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000).$$

Computing syndrome of e gives

$$S = eH^T = (S_1, S_2) = (00100, 1100).$$

Since the first $n_1(= 2)$ bits of S_1 are all-zero and the remaining $n_2(= 4)$-bits form a non-zero pattern, therefore, we infer that the error lies in the second sector of the error vector.

We form a new syndrome vector

$$S^* = (S_1^*, S_2^*),$$

where

$$\begin{aligned} S_1^* &= n_2(i.e.4)\text{-bit non-zero pattern in } S_1 = 1100 = \alpha^4, \\ S_2^* &= \text{first 4-bits of } S_2 = 1100 = \alpha^4, \end{aligned}$$

where α is a root of $x^4 + x + 1$.

Thus

$$S^* = (S_1^*, S_2^*) = (\alpha^4, \alpha^4)$$

The error locator polynomial $\sigma^*(x)$ for the syndrome S^* using the Berlekamp-Massey algorithm is computed as

$$\sigma^*(x) = 1 + x.$$

Since $\deg(\sigma^*(x_1) = 1$, therefore, we infer that there is only one erroneous i-byte in the erroneous second sector. Since $\alpha^0 = 1$ is a root of $\sigma^*(x)$, therefore, $\alpha_0^{-1} = 1 = \alpha^0$ gives the location of the erroneous i-byte i.e. 0^{th} i-byte in the second sector contains errors.

The evaluator polynomial $Z^*(x)$ is given by

$$\begin{aligned} Z^*(x) &= \sigma^*(x)S^*(x) \\ &= (1+x)(1+\alpha^4 x + \alpha^4 x^2) \\ &= 1 + \alpha x \text{ (as } \deg(Z^*(x) \leq 1). \end{aligned}$$

Now, the erroneous i-byte pattern is given by the formula

$$\begin{aligned} e_2^0 &= \beta_0 \left(\frac{Z^*(\beta_0^{-1})}{1} \right), \\ &= \alpha^0 \left(\frac{1 + \alpha.1}{1} \right) = 1 + \alpha = \alpha^4 = (1100), \quad \text{where } \beta_0 = \alpha^0 = 1. \end{aligned}$$

Hence the error pattern is given by

$$e = (00\ \ 00\ \ 00\ \vdots\ 1100\ \ 0000\ \ 0000\ \ 0000\ \ 0000\ \ 0000\ \ 0000\ \ 0000\ \ 0000\ \ 0000$$
$$0000\ 0000\ 0000\ 0000\ 0000).$$

Comparative Study.

In this section, we present a comparative study of rates of transmission/storage of binary uniformly independent i-spotty byte error control codes presented in this paper and non-uniformly independent i-spotty byte codes presented earlier [4,5] for different values of the parameters $n_1, n_2, \cdots, n_s$ and $t_1, t_2 \cdots, t_s$. We are restricting ourself for $s = 2$ only.

Table 5.1

Value of parameters	measures μ *of* uniformly independent errors to be corrected	Rate of uniformly independent i-spotty byte code	Rate of non-uniformly independent i-spotty byte code
$n_1 = 2, n_2 = 3$ $t_1 = 2, t_2 = 2$	$\mu = 1$	0.703	0.600
$n_1 = 3, n_2 = 4$ $t_1 = 3, t_2 = 3$	$\mu = 1$	0.864	0.816
$n_1 = 3, n_2 = 5$ $t_1 = 2, t_2 = 4$	$\mu = 1$	0.926	0.900
$n_1 = 2, n_2 = 4$ $t_1 = 2, t_2 = 3$	$\mu = 1$	0.848	0.785
$n_1 = 2, n_2 = 3$ $t_1 = 2, t_2 = 1$	$\mu = 2$	0.481	0.333
$n_1 = 3, n_2 = 4$ $t_1 = 1, t_2 = 1$	$\mu = 2$	0.764	0.523
$n_1 = 3, n_2 = 3$ $t_1 = 1, t_2 = 1$	$\mu = 2$	0.642	0.440

We infer from the Table 5.1 that the rate of transmission/storage of uniformly independent i-spotty byte codes is higher than the non-uniformly independent i-spotty byte codes and thus the codes presented in this paper are more economical to use and provide better transmission/storage rate than the earlier considered non-uniformly independent i-spotty-byte codes [4,5].

5. Conclusion.

In this paper, we have presented a new class of i-spotty-byte codes viz. uniformly independent i-spotty-byte error control codes which are capable of correcting all uniform i-spotty-byte errors and the errors are independent in the sense that the sum of erroneous i-bytes occuring in the erroneous sector is non-zero. We have discussed the code design of these codes in terms of their parity check matrix followed by a decoding algorithm to decode the received vector which is further illustrated by several examples. Finally, a comparative study of the codes presented in this paper with the earlier known i-spotty-byte codes has been given to show that these codes are more economical in terms of their transmission/storage than the previously considered i-spotty-byte codes [4,5].

Acknowledgment. The author would like to thank her spouse Prof.(Dr.) Arihant Jain for his constant support and encouragement for pursuing research.

References

[1] E. Fujiwara, Codes for dependable systems, Wiley Interscience, 2006.

[2] S. Jain, *Irregular-spotty-byte error control codes*, World Applied Sciences Journal, 30 (2014), 1993-1999.

[3] S. Jain, *On weight enumerators of i-spotty-byte codes*, World Applied Sciences Journal, 30 (2014), 1985-1992.

[4] S. Jain, *Code design of i-spotty-byte error correcting codes*, Alexendria Journal of Mathematics, 5 (2015), 20-42.

[5] S. Jain, *Uniform i-spotty-byte error control codes*, Journal of Combinatorial Mathematics and Combinatorial Computing, 100 (2017), 77-95.

[6] K. Suzuki, T. Kashiyama and E. Fujiwara, *A General class of M-spotty Byte Error Control Codes*, IEICE Trans. Fundamentals, Vol.-E90-A, No.7, July (2007).

[7] K. Suzuki, T. Kashiyama and E. Fujiwara, *Complex m-spotty Byte Error Control Codes*, Por. IEEE Inform. Theory Workshop:211-215, 2005.

[8] K. Suzuki, M. Shimizu, T. Kashiyama and E. Fujiwara, *A Class of Error Control Codes for m-spotty Byte Errors occured in a limited number of Bytes*, Proc. IEEE Int. Symp. on Information Theory:2109-2113, 2005.

ALGEBRAS GROUPS AND GEOMETRIES

INDEX VOL. 35, 2018

THE GEOMETRY OF A SPECIAL CLASS OF CURVES ON THE HYPERBOLOID MODEL H*(r) OF THE LORENTZ – MINKOWSKI 3-SPACE IR_1^3, 1

Mehmet Aydınalp
Manisa Celal Bayar University
Faculty of Arts and Sciences, Department of Mathematics
45140, Manisa, Turkey
Hasan Hüseyin Uğurlu
Gazi University, Faculty of Education, Department of Secondary Education
Science and Mathematics Teaching, Mathematics Teaching Program
06560, Ankara, Turkey

NEWTONIAN GRAVITATIONAL RADIATION AND WAVES, 21

Gustavo V. López
Departamento de Física, Universidad de Guadalajara
Blvd. Marcelino García Barragan y Calzada Olímpica
44200 Guadalajara, Jalisco, Mexico

SET-THEORETIC GENERATORS FOR RATIONAL SPHERICAL CURVES, 29

Haohao Wang
Department of Mathematics
Southeast Missouri State University
Cape Girardeau, MO 63701 U.S.A.
Ron Goldman
Department of Computer Science
Rice University
Houston, TX 77251 U.S.A.

ISODUAL THEORY OF ANTIMATTER, I: MATHEMATICAL AND PHYSICAL METHODS, 67

Arun S. Muktibodh
Mohota College of Science
Nagpur-440009, India
The Institute for Basic Research
Florida, U.S.A.

A PHYSICAL THEORY OF DYNAMICS WITH THE INVARIANCE OF A SIXTEEN-DIMENSIONAL ALGEBRA, 93
Simon Davis
Research Foundation of Southern California
8837 Villa La Jolla Drive #13595
La Jolla, CA 92309
A TRIALITY GROUP OF NONASSOCIATIVE ALGEBRAS WITH INVOLUTION, 113
Noriaki Kamiya
Department of Mathematics, University of Aizu
Aizuwakamatsu, Japan
Susumu Okubo
Department of Physics and Astronomy, University of Rochester
Rochester, NY, USA
FOUR INDEPENDENT EIGENVECTORS AND THEIR PROPERTIES FOR THE PROBLEM OF ACOUSTIC 4P-SH-WAVE PROPAGATION INCORPORATING GRAVITATIONAL PHENOMENA, 169
Aleksey Anatolievich Zakharenko
International Institute of Zakharenko Waves (IIZWs)
660014, ul. Chaikovskogo, 20-304, Krasnoyarsk, Russia
ON n-MULTIPLICATIVE HIGHER DERIVATIONS ON ALTERNATIVE RINGS, 205
João Carlos da Motta Ferreira and
Maria das Graças Bruno Marietto
Center of Mathematics, Computation and Cognition,
Federal University of ABC
Santa Adélia Street, 166,
09210-170, Santo André, Brazil
CHARACTERIZATION OF ADDITIVE n-MULTIPLICATIVE HIGHER DERIVATIONS OF NONASSOCIATIVE ALGEBRAS, 215
João Carlos da Motta Ferreira and
Maria das Graças Bruno Marietto
Center for Mathematics, Computation and Cognition,
Federal University of ABC
Santa Adélia Street, 166,
09210-170, Santo André, Brazil
ON SURFACE MEASURES OF CONVEX BODIES AND GENERALIZATIONS OF KNOWN TANGENTIAL IDENTITIES, 231
J. Aspegren
Havukantie 6,
95450 Tornio, Finland

ZUR THEORIE DER q, ω-LIESCHEN MATRIXGRUPPEN, 243
Thomas Ernst
Department of Mathematics, Uppsala University
P.O. Box 480, SE-751 06 Uppsala, Sweden
(ε, δ)-FREUDENTHAL KANTOR TRIPLE SYSTEMS, δ-STRUCTURABLE ALGEBRAS AND LIE SUPERALGEBRAS, 267
Noriaki Kamiya
Center for Mathematical Sciences, University of Aizu
965-8580, Aizuwakamatsu, Japan
Daniel Mondoc
Centre for Mathematical Sciences, Lund University
22 100 Lund, Sweden
Susumu Okubo
Department of Physics, University of Rochester
Rochester, NY 14627
FOUR INDEPENDENT EIGENVECTORS AND THEIR PROPERTIES FOR THE PROBLEM OF ACOUSTIC 4P-SH-WAVE PROPAGATION INCORPORATING GRAVITATIONAL PHENOMENA, 283
Aleksey Anatolievich Zakharenko
International Institute of Zakharenko Waves (IIZWs)
660014, ul. Chaikovskogo, 20-304
Krasnoyarsk, Russia
METRIC TENSOR IS GROUPOID, 319
Zbigniew Oziewicz
Universidad Nacional Autónoma de México
Facultad de Estudios Superiores Cuautitlán
ADDITIVITY OF JORDON n-TUPLE HIGHER DERIVABLE MAPS ON RINGS, 329
João Carlos da Motta Ferreira and Maria das Graças Bruno Marietto
Center for Mathematics, Computation and Cognition,
Federal University of ABC
Santa Adélia Street, 166, 09210-170, Santo André, Brazil
RINGS IN WHICH ELEMENTS ARE A SUM OF A CENTRAL AND NILPOTENT ELEMENT, 347
Yosum Kurtlmaz
Department of Mathematics, Bilkent University, Ankara, Turkey
Abdullah Harmanci
Department of Mathematics, Hacettepe University, Ankara, Turkey
HAMILTON-JACOBI TREATMENT OF SUPERSTRING AND QUANTIZATION OF FIELDS WITH CONSTRAINTS, 365
W. I. Eshraim
Institute for Theoretical Physics, Goethe University, Frankfurt am Main,
Institute for Theoretical Physics, Justus-Liebig University,
Giessen, Germany

ON RIEMANN CONJECTURE, 389
Jiang Yu
Guangzeng Group, fourth floor, number 10,
Guangming East Road, Zengcheng City,
Post Code: 511316, Guangdong Province, China
ISONUMBERS AND RGB IMAGE ENCRYPTION, 395
Mamadou I. Wade and Tepper L. Gill
EECS Howard University, Washington, DC 20059
ON EXTENDED CAMPOPIANO'S TYPE BOUND FOR LPA CODES, 413
Sapna Jain
Shanxi Normal University, P. R. China
K. P. Shum
Institute of Mathematics, Yunnan University, Kunming, 650091
P. R. China
UNIFORMLY INDEPENDENT I-SPOTTY-BYTE ERROR CONTROL CODES, 427
Sapna Jain
Shanxi Normal University, P. R. China